Enterasys® Wireless

Controller, Access Points and Convergence Software

CLI Reference Guide

Version 7.41

P/N 9034529-04

enterasys®

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

© 2011 Enterasys Networks, Inc. All rights reserved.

Part Number: 9034529-04 April 2011

ENTERASYS, ENTERASYS NETWORKS, ENTERASYS SECURE NETWORKS, NETSIGHT, ENTERASYS NETSIGHT, and any logos associated therewith, are trademarks or registered trademarks of Enterasys Networks, Inc., in the United States and/or other countries. For a complete list of Enterasys trademarks, see http://www.enterasys.com/company/trademarks.aspx.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

Documentation URL: https://extranet.enterasys.com/downloads

Enterasys Networks, Inc. Software License Agreement

This document is an agreement ("Agreement") between You, the end user, and Enterasys Networks, Inc. on behalf of itself and its Affiliates ("Enterasys") that sets forth your rights and obligations with respect to the software contained in CD-ROM or other media. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. BY INSTALLING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, INC. (978) 684-1000. Attn: Legal Department.

Enterasys will grant You a non-transferable, non-exclusive license to use the machine-readable form of software (the "Licensed Software") and the accompanying documentation (the Licensed Software, the media embodying the Licensed Software, and the documentation are collectively referred to in this Agreement as the "Licensed Materials") on one single computer if You agree to the following terms and conditions:

1. **TERM.** This Agreement is effective from the date on which You open the package containing the Licensed Materials. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and your license to use the Licensed Materials will also terminate if You fail to comply with any term or condition herein.

2. **GRANT OF SOFTWARE LICENSE.** The license granted to You by Enterasys when You open this sealed package authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

3. **RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS**. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Enterasys' prior written consent, and in no event shall You operate more than one copy of the Licensed Software. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement.

You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

4. **TITLE AND PROPRIETARY RIGHTS**.

   (a) The Licensed Materials are copyrighted works and are the sole and exclusive property of Enterasys, any company or a division thereof which Enterasys controls or is controlled by, or which may result from the merger or consolidation with Enterasys (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

   (b) You further acknowledge that in the event of a breach of this Agreement, Enterasys shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Enterasys shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Enterasys.

5. **PROTECTION AND SECURITY**. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Enterasys relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Enterasys' exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Enterasys' prior written approval, and shall return such information and data to Enterasys at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Enterasys or of information which has been or subsequently is made public by Enterasys, or a third party having authority to do so.

You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Enterasys or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Enterasys. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Enterasys of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Enterasys or its Affiliates and/or its/their software suppliers.

6. **MAINTENANCE AND UPDATES**. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Enterasys Service and Maintenance Agreement, if Enterasys and You enter into such an agreement. Except as specifically set forth in such agreement, Enterasys shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

7. **DEFAULT AND TERMINATION**. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Enterasys, or in the event that You become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Enterasys may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Enterasys and You.

(a) Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Enterasys the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Enterasys.

(b) Sections 4, 5, 7, 8, 9, 10, 11, and 12 shall survive termination of this Agreement for any reason.

8. **EXPORT REQUIREMENTS**. You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Licensed Materials are exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Licensed Materials and agree that You will use the Licensed Materials for civil end uses only and not for military purposes.

If the Licensed Materials are exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Section 4 of this Agreement, You agree not to (i) reexport or release the Licensed Software, the source code for the Licensed Software or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Cambodia, Cuba, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Libya, Macau, Moldova, Mongolia, North Korea, the People's Republic of China, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Licensed Software or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant o r any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

9. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS**. The Licensed Materials (i) were developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

10. **LIMITED WARRANTY AND LIMITATION OF LIABILITY**. The only warranty Enterasys makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Enterasys in good faith determines that the media and proof of payment of the license fee are returned to Enterasys or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.

NEITHER ENTERASYS NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL ENTERASYS OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF ENTERASYS OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ENTERASYS OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

11. **JURISDICTION**. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the Commonwealth of Massachusetts, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

12. **GENERAL**.

(a) This Agreement is the entire agreement between Enterasys and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.

(b) This Agreement may not be changed or amended except in writing signed by both parties hereto.

(c) You represent that You have full right and/or authorization to enter into this Agreement.

(d) This Agreement shall not be assignable by You without the express written consent of Enterasys, The rights of Enterasys and Your obligations under this Agreement shall inure to the benefit of Enterasys' assignees, licensors, and licensees.

(e) Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

(f) The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

(g) Enterasys' waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

(h) Should You have any questions regarding this Agreement, You may contact Enterasys at the address set forth below. Any notice or other communication to be sent to Enterasys must be mailed by certified mail to the following address: ENTERASYS NETWORKS, INC., 50 Minuteman Road, Andover, MA 01810 Attn: Manager - Legal Department.

Contents

About This Guide

Who Should Use This Guide xxi
How to Use This Guide xxi
Related Documentation xxii
Formatting Conventions xxii
Keyboard Shortcuts xxiii
Getting Help xxiii

Chapter 1: CLI Structure

Account Types 1-1

Chapter 2: Common Commands

2.1 apply 2-1
2.2 end 2-1
2.3 exit 2-2
2.4 help 2-2
2.5 logout 2-3
2.6 no 2-3
2.7 show 2-3

Chapter 3: root Commands

3.1 audit 3-3
3.2 availability 3-3
3.2.1 pair 3-3
3.2.2 pairip 3-4
3.2.3 pairrole 3-4
3.2.4 fast_failover 3-4
3.2.5 link_timeout 3-5
3.2.6 sync-config 3-5
3.2.7 sync-mu 3-6
3.3 backup 3-6
3.4 copy 3-7
3.5 host-attributes 3-8
3.5.1 hostname 3-9
3.5.2 domain 3-9
3.5.3 dns 3-10
3.5.3.1 dns 3-10
3.5.3.2 move 3-10
3.6 export 3-11
3.7 flash 3-13
3.8 no flash 3-13
3.9 healthpoll 3-14
3.10 import 3-14
3.11 key 3-15
3.11.1 activate 3-15
3.11.2 ecap 3-15
3.11.3 extcp 3-16
3.12 lanset 3-16
3.13 loglevel 3-17
3.14 ping 3-18

3.15 radtest 3-19
3.16 radtest_mba 3-20
3.17 reset 3-20
3.18 restart 3-22
3.19 restore 3-22
3.20 secureconnection 3-23
3.20.1 secret 3-23
3.21 show 3-23
3.21.1 show ac version 3-23
3.21.2 show active-user 3-24
3.21.3 show ap 3-24
3.21.4 show ap_certificate 3-28
3.21.5 show ap_certreq 3-28
3.21.6 show ap_inventory 3-28
3.21.7 show apup 3-30
3.21.8 show audits 3-31
3.21.9 show availability 3-32
3.21.10 show backup 3-32
3.21.11 show bootrom 3-33
3.21.12 show cdrs 3-33
3.21.13 show checkpoint 3-35
3.21.14 show clients apserial 3-35
3.21.15 show clients vns 3-36
3.21.16 show run-config 3-37
3.21.17 show dns 3-37
3.21.18 show export 3-37
3.21.19 show flash 3-38
3.21.20 show healthpoll 3-38
3.21.21 show import 3-39
3.21.22 show import_status 3-39
3.21.23 show key 3-40
3.21.24 show l2ports 3-40
3.21.25 show lanset 3-41
3.21.26 show log 3-42
3.21.27 show loglevel 3-44
3.21.28 show ospf 3-44
3.21.29 show policy 3-46
3.21.30 show wlans 3-46
3.21.31 show report 3-47
3.21.32 show restore 3-50
3.21.33 show routes 3-50
3.21.34 show schedule_ backup 3-51
3.21.35 show schedule_upgrade 3-51
3.21.36 show snmp 3-52
3.21.37 show stats 3-52
3.21.38 show syslog 3-55
3.21.39 show system_state 3-56
3.21.40 show tech_support 3-58
3.21.41 show time 3-58
3.21.42 show time-config 3-59
3.21.43 show topology 3-59
3.21.44 show traffic_capture 3-60
3.21.45 show upgrade 3-61
3.21.46 show upgrade_backup_dest 3-61
3.21.47 show upgrade_history 3-61
3.21.48 show upgrade_image_src 3-62

3.21.49 show users 3-62
3.21.50 show vnsmode 3-62
3.21.51 show vnsmode radius 3-63
3.21.52 show web 3-64
3.22 shutdown 3-64
3.23 tech_support 3-64
3.24 traceroute 3-65
3.25 upgrade 3-67
3.25.1 upgrade ac 3-67
3.25.2 upgrade apup 3-68
3.26 upgrade_backup_dest 3-69
3.27 upgrade_image_src 3-69

Chapter 4: ap Commands

4.1 access 4-1
4.2 blacklist 4-2
4.2.1 export 4-2
4.2.2 import 4-3
4.2.3 mac 4-3
4.2.4 mac-list-mode 4-4
4.3 defaults 4-4
4.3.1 11n 4-5
4.3.1.1 bcast_disassoc 4-5
4.3.1.2 client_session 4-6
4.3.1.3 country 4-6
4.3.1.4 lbs-status 4-7
4.3.1.5 led-mode 4-7
4.3.1.6 lldp 4-7
4.3.1.7 persistent 4-8
4.3.1.8 poll_timeout 4-9
4.3.1.9 radio1 4-9
4.3.1.9.1 admin-mode 4-10
4.3.1.9.2 antsel 4-10
4.3.1.9.3 atpc 4-11
4.3.1.9.4 beaconp 4-11
4.3.1.9.5 dcs 4-12
4.3.1.9.5.1 channel_plan 4-12
4.3.1.9.5.2 mode 4-13
4.3.1.9.5.3 noise_threshold 4-13
4.3.1.9.5.4 occupancy_threshold 4-14
4.3.1.9.5.5 radio_channels 4-14
4.3.1.9.5.6 update_period 4-15
4.3.1.9.6 domain 4-15
4.3.1.9.7 dtim 4-16
4.3.1.9.8 frag 4-16
4.3.1.9.9 max-distance 4-17
4.3.1.9.10 minbrate 4-17
4.3.1.9.11 mode 4-18
4.3.1.9.12 n_addba_support 4-18
4.3.1.9.13 n_aggr_mpdu 4-19
4.3.1.9.14 n_aggr_mpdu_max 4-19
4.3.1.9.15 n_aggr_mpdu_max_subframes 4-19
4.3.1.9.16 n_aggr_msdu 4-20
4.3.1.9.17 n_aggr_msdu_max 4-20
4.3.1.9.18 n_chlbonding 4-21

4.3.1.9.19 n_chlwidth 4-21
4.3.1.9.20 n_guardinterval 4-22
4.3.1.9.21 n_pbthreshold 4-22
4.3.1.9.22 n_pmode 4-22
4.3.1.9.23 n_poffset 4-23
4.3.1.9.24 n_ptype 4-23
4.3.1.9.25 rts 4-23
4.3.1.9.26 tx_adjust_power 4-24
4.3.1.9.27 tx_max_power 4-24
4.3.1.9.28 tx_min_power 4-25
4.3.1.10 radio2 4-25
4.3.1.10.1 admin-mode 4-26
4.3.1.10.2 antsel 4-26
4.3.1.10.3 atpc 4-27
4.3.1.10.4 beaconp 4-27
4.3.1.10.5 dcs 4-28
4.3.1.10.5.1 channel_plan 4-28
4.3.1.10.5.2 mode 4-29
4.3.1.10.5.3 radio_channels 4-29
4.3.1.10.6 domain 4-30
4.3.1.10.7 dtim 4-30
4.3.1.10.8 frag 4-30
4.3.1.10.9 max-distance 4-31
4.3.1.10.10 minbrate 4-31
4.3.1.10.11 mode 4-32
4.3.1.10.12 n_addba_support 4-33
4.3.1.10.13 n_aggr_mpdu 4-33
4.3.1.10.14 n_aggr_mpdu_max 4-34
4.3.1.10.15 n_aggr_mpdu_max_subframes 4-34
4.3.1.10.16 n_aggr_msdu 4-34
4.3.1.10.17 n_aggr_msdu_max 4-35
4.3.1.10.18 n_chlbonding 4-35
4.3.1.10.19 n_chlwidth 4-36
4.3.1.10.20 n_guardinterval 4-36
4.3.1.10.21 n_pbthreshold 4-36
4.3.1.10.22 n_pmode 4-37
4.3.1.10.23 n_poffset 4-37
4.3.1.10.24 n_ptype 4-38
4.3.1.10.25 pmode 4-38
4.3.1.10.26 prate 4-39
4.3.1.10.27 preamble 4-39
4.3.1.10.28 ptype 4-39
4.3.1.10.29 rts 4-40
4.3.1.10.30 tx_max_power 4-40
4.3.1.11 show 4-41
4.3.2 4102 4-41
4.3.2.1 bcast_disassoc 4-41
4.3.2.2 client_session 4-42
4.3.2.3 country 4-42
4.3.2.4 led-mode 4-43
4.3.2.5 lldp 4-43
4.3.2.6 persistent 4-44
4.3.2.7 poll_timeout 4-44
4.3.2.8 radio1 4-45
4.3.2.8.1 admin-mode 4-46
4.3.2.8.2 atpc 4-46

4.3.2.8.3 beaconp 4-46
4.3.2.8.4 dcs 4-47
4.3.2.8.4.1 channel_plan 4-47
4.3.2.8.4.2 mode 4-48
4.3.2.8.4.3 radio_channels 4-48
4.3.2.8.5 divrx 4-49
4.3.2.8.6 divtx 4-49
4.3.2.8.7 domain 4-50
4.3.2.8.8 dtim 4-50
4.3.2.8.9 frag 4-51
4.3.2.8.10 hwretries 4-51
4.3.2.8.11 maxbrate 4-52
4.3.2.8.12 maxoprate 4-52
4.3.2.8.13 max-distance 4-52
4.3.2.8.14 minbrate 4-53
4.3.2.8.15 mode 4-53
4.3.2.8.16 rts 4-54
4.3.2.8.17 tx_adjust_power 4-54
4.3.2.8.18 tx_max_power 4-55
4.3.2.8.19 tx_min_power 4-55
4.3.2.9 radio2 4-55
4.3.2.9.1 admin-mode 4-56
4.3.2.9.2 atpc 4-56
4.3.2.9.3 beaconp 4-57
4.3.2.9.4 dcs 4-57
4.3.2.9.4.1 channel_plan 4-57
4.3.2.9.4.2 mode 4-58
4.3.2.9.4.3 radio_channels 4-58
4.3.2.9.5 divrx 4-59
4.3.2.9.6 divtx 4-59
4.3.2.9.7 domain 4-60
4.3.2.9.8 dtim 4-60
4.3.2.9.9 frag 4-61
4.3.2.9.10 hwretries 4-61
4.3.2.9.11 maxbrate 4-62
4.3.2.9.12 max-distance 4-62
4.3.2.9.13 maxoprate 4-63
4.3.2.9.14 minbrate 4-63
4.3.2.9.15 mode 4-63
4.3.2.9.16 pmode 4-64
4.3.2.9.17 prate 4-64
4.3.2.9.18 preamble 4-65
4.3.2.9.19 ptype 4-65
4.3.2.9.20 rts 4-66
4.3.2.9.21 tx_max_power 4-66
4.3.2.10 telnet 4-66
4.3.3 assign 4-67
4.3.3.1 wlans-list 4-67
4.3.4 dualband 4-67
4.3.4.1 bcast_disassoc 4-68
4.3.4.2 client_session 4-68
4.3.4.3 country 4-69
4.3.4.4 led-mode 4-69
4.3.4.5 lldp 4-70
4.3.4.6 persistent 4-70
4.3.4.7 poll_timeout 4-71

4.3.4.8 radio1 4-71
4.3.4.8.1 admin-mode 4-72
4.3.4.8.2 atpc 4-72
4.3.4.8.3 beaconp 4-73
4.3.4.8.4 dcs 4-73
4.3.4.8.4.1 channel_plan 4-73
4.3.4.8.4.2 mode 4-74
4.3.4.8.4.3 noise_threshold 4-75
4.3.4.8.4.4 occupancy_threshold 4-75
4.3.4.8.4.5 radio_channels 4-75
4.3.4.8.4.6 update_period 4-76
4.3.4.8.5 divrx 4-77
4.3.4.8.6 divtx 4-77
4.3.4.8.7 domain 4-77
4.3.4.8.8 dtim 4-78
4.3.4.8.9 frag 4-78
4.3.4.8.10 hwretries 4-79
4.3.4.8.11 max-distance 4-79
4.3.4.8.12 maxbrate 4-80
4.3.4.8.13 maxoprate 4-80
4.3.4.8.14 minbrate 4-81
4.3.4.8.15 mode 4-81
4.3.4.8.16 rts 4-82
4.3.4.8.17 tx_adjust_power 4-82
4.3.4.8.18 tx_max_power 4-82
4.3.4.8.19 tx_min_power 4-83
4.3.4.9 radio2 4-83
4.3.4.9.1 admin-mode 4-84
4.3.4.9.2 atpc 4-84
4.3.4.9.3 beaconp 4-85
4.3.4.9.4 dcs 4-85
4.3.4.9.4.1 channel_plan 4-85
4.3.4.9.4.2 mode 4-86
4.3.4.9.4.3 noise_threshold 4-87
4.3.4.9.4.4 occupancy_threshold 4-87
4.3.4.9.4.5 radio_channels 4-87
4.3.4.9.4.6 update_period 4-88
4.3.4.9.5 divrx 4-88
4.3.4.9.6 divtx 4-89
4.3.4.9.7 domain 4-89
4.3.4.9.8 dtim 4-90
4.3.4.9.9 frag 4-90
4.3.4.9.10 hwretries 4-90
4.3.4.9.11 maxbrate 4-91
4.3.4.9.12 maxoprate 4-91
4.3.4.9.13 minbrate 4-92
4.3.4.9.14 mode 4-92
4.3.4.9.15 pmode 4-93
4.3.4.9.16 prate 4-93
4.3.4.9.17 preamble 4-94
4.3.4.9.18 ptype 4-94
4.3.4.9.19 rts 4-94
4.3.4.9.20 tx_adjust_power 4-95
4.3.4.9.21 tx_max_power 4-95
4.3.4.9.22 tx_min_power 4-96
4.3.4.10 telnet 4-96

4.3.5 learnac 4-97
4.3.6 std 4-97
4.3.6.1 bcast_disassoc 4-97
4.3.6.2 client_session 4-98
4.3.6.3 country 4-98
4.3.6.4 led-mode 4-99
4.3.6.5 lldp 4-99
4.3.6.6 persistent 4-100
4.3.6.7 poll_timeout 4-100
4.3.6.8 radio1 4-101
4.3.6.8.1 admin-mode 4-101
4.3.6.8.2 atpc 4-102
4.3.6.8.3 beaconp 4-102
4.3.6.8.4 dcs 4-103
4.3.6.8.4.1 channel_plan 4-103
4.3.6.8.4.2 mode 4-103
4.3.6.8.4.3 radio_channels 4-104
4.3.6.8.5 divrx 4-105
4.3.6.8.6 divtx 4-105
4.3.6.8.7 domain 4-106
4.3.6.8.8 dtim 4-106
4.3.6.8.9 frag 4-106
4.3.6.8.10 hwretries 4-107
4.3.6.8.11 maxbrate 4-108
4.3.6.8.12 maxoprate 4-108
4.3.6.8.13 max-distance 4-108
4.3.6.8.14 minbrate 4-109
4.3.6.8.15 mode 4-109
4.3.6.8.16 rts 4-110
4.3.6.8.17 tx_max_power 4-110
4.3.6.9 radio2 4-111
4.3.6.9.1 admin-mode 4-111
4.3.6.9.2 atpc 4-112
4.3.6.9.3 beaconp 4-112
4.3.6.9.4 dcs 4-112
4.3.6.9.4.1 channel_plan 4-113
4.3.6.9.4.2 mode 4-113
4.3.6.9.4.3 radio_channels 4-114
4.3.6.9.5 divrx 4-114
4.3.6.9.6 divtx 4-114
4.3.6.9.7 domain 4-115
4.3.6.9.8 dtim 4-115
4.3.6.9.9 frag 4-116
4.3.6.9.10 hwretries 4-116
4.3.6.9.11 maxbrate 4-117
4.3.6.9.12 max-distance 4-117
4.3.6.9.13 maxoprate 4-118
4.3.6.9.14 minbrate 4-118
4.3.6.9.15 mode 4-119
4.3.6.9.16 pmode 4-119
4.3.6.9.17 prate 4-120
4.3.6.9.18 preamble 4-120
4.3.6.9.19 ptype 4-120
4.3.6.9.20 rts 4-121
4.3.6.9.21 tx_max_power 4-121
4.3.6.10 telnet 4-122

4.4 export_drm 4-122
4.5 import_drm 4-123
4.6 load-groups 4-124
4.6.1 create 4-124
4.6.2 delete 4-125
4.6.3 <named-load-group> 4-126
4.6.3.1 assign-ap 4-126
4.6.3.2 assign-radio 4-126
4.6.3.3 assign-wlan 4-127
4.6.3.4 bandpreference 4-128
4.6.3.5 loadcontrol 4-128
4.6.3.6 name 4-128
4.6.3.7 radio-load 4-129
4.6.3.8 show 4-130
4.6.4 show 4-130
4.7 maintenance 4-131
4.7.1 upgrd 4-131
4.8 registration 4-131
4.8.1 cluster-encryption 4-132
4.8.2 cluster-inter-ap-roam 4-132
4.8.3 cluster-shared-secret 4-132
4.8.4 dinterval 4-133
4.8.5 dretry 4-133
4.8.6 passwd 4-134
4.8.7 security 4-134
4.8.8 sshpasswd 4-135
4.9 remove 4-135
4.10 search 4-136
4.11 serial 4-136
4.12 <serial> 4-137
4.12.1 leftantenna-radio2 4-138
4.12.2 rightantenna-radio2 4-138
4.12.3 antennaleft 4-139
4.12.4 antennamiddle 4-140
4.12.5 antennaright 4-140
4.12.6 leftantenna-radio1 4-141
4.12.7 rightantenna-radio1 4-142
4.12.8 antennaleftmiddle 4-142
4.12.9 antennarightmiddle 4-143
4.12.10 apip 4-144
4.12.11 bgway 4-144
4.12.12 802_1x 4-144
4.12.12.1 eap 4-145
4.12.12.2 gen_certreq 4-145
4.12.12.3 peap 4-146
4.12.13 aclist 4-146
4.12.14 bcast_disassoc 4-147
4.12.15 client_session 4-147
4.12.16 country 4-147
4.12.17 desc 4-148
4.12.18 lbs-status 4-148
4.12.19 led-mode 4-148
4.12.20 location 4-149
4.12.21 lldp 4-150
4.12.22 move 4-150
4.12.23 name 4-151

4.12.24 persistent ... 4-151
4.12.25 poll_timeout ... 4-152
4.12.26 port-setting ... 4-152
4.12.27 radio1 ... 4-152
4.12.28 radio2 ... 4-153
4.12.29 role ... 4-153
4.12.30 show ... 4-153
4.12.31 ssh ... 4-154
4.12.32 telnet ... 4-154
4.12.33 tunnel-mtu ... 4-155
4.12.34 usedhcp ... 4-155
4.12.35 vlanid ... 4-156
4.12.36 wlan ... 4-156

Chapter 5: checkpoint Commands

5.1 cpip ... 5-1
5.2 cplog ... 5-2
5.3 cpcert ... 5-3
5.4 elalogint ... 5-3
5.5 elaport ... 5-3
5.6 elaq ... 5-4
5.7 elaretry ... 5-4
5.8 sicname ... 5-5
5.9 sicpwd ... 5-5

Chapter 6: l2ports Commands

6.1 esaN ... 6-1
6.2 pc.N ... 6-1
6.3 portN ... 6-1
6.3.1 port ... 6-2
6.4 show ... 6-2

Chapter 7: ip Commands

7.1 route ... 7-1
7.2 ospf ... 7-2
7.2.1 area ... 7-2
7.2.2 areatype ... 7-3
7.2.3 routerid ... 7-3
7.2.4 status ... 7-4
7.2.5 ospfinterface ... 7-4
7.2.5.1 <n> ... 7-4
7.2.5.2 authkey ... 7-5
7.2.5.3 authtype ... 7-5
7.2.5.4 deadinterval ... 7-6
7.2.5.5 hellointerval ... 7-6
7.2.5.6 linkcost ... 7-6
7.2.5.7 retransmitinterval ... 7-7
7.2.5.8 status ... 7-7
7.2.5.9 transmitdelay ... 7-7

Chapter 8: login Commands

8.1 apply ... 8-1
8.2 auth ... 8-2
8.2.1 server ... 8-2

8.2.2 primary 8-2
8.2.3 authset 8-3
8.2.4 move 8-3
8.2.5 radtest_login 8-4
8.3 auth-order 8-4
8.4 move 8-5
8.5 show 8-6

Chapter 9: mitigator Commands

9.1 analysis 9-1
9.2 wcswip 9-2
9.3 scgroup 9-2
9.3.1 sgname 9-3
9.3.2 <scan group name> 9-3
9.3.2.1 aplist 9-4
9.3.2.2 interval 9-4
9.3.2.3 dtime 9-4
9.3.2.4 radio 9-5
9.3.2.5 type 9-5
9.3.2.6 channel 9-6
9.3.2.7 start 9-6
9.3.2.8 show 9-6
9.4 friend 9-7
9.4.1 frlist 9-7

Chapter 10: mobility Commands

10.1 mrole 10-1
10.2 mport 10-2
10.3 mheartbeat 10-2
10.4 slpreg 10-2
10.5 agent 10-3
10.6 secmode 10-3
10.7 mdismethod 10-4
10.8 mmanagerip 10-4

Chapter 11: schedule_backup Commands

11.1 dir 11-2
11.2 freq 11-2
11.3 password 11-3
11.4 protocol 11-3
11.5 server 11-4
11.6 starttime 11-4
11.7 type 11-4
11.8 user 11-5

Chapter 12: schedule_upgrade Commands

12.1 schld_upgrd 12-1
12.2 upgrade_backup 12-2

Chapter 13: snmp Commands

13.1 contact 13-1
13.2 context 13-2
13.3 enable 13-2
13.4 engine-id 13-3

13.5 location 13-3
13.6 port 13-4
13.7 publish-ap 13-4
13.8 rcommunity 13-5
13.9 rwcommunity 13-5
13.10 severity 13-5
13.11 show 13-6
13.12 trap-manager-v1v2 13-6
13.13 trap-manager-v3 13-7
13.14 user 13-7

Chapter 14: syslog Commands
14.1 audmsg 14-1
14.2 facility 14-1
14.3 svcmsg 14-2
14.4 syslogip 14-3

Chapter 15: time Commands
15.1 clock 15-1
15.2 date 15-2
15.3 ntp 15-2
15.4 ntpip 15-3
15.5 tz 15-3

Chapter 16: traffic_capture Commands
16.1 file_name 16-1
16.2 size 16-2
16.3 destination 16-2
16.4 interface 16-3
16.5 delete 16-3
16.6 list 16-4
16.7 start 16-4
16.8 stop 16-5
16.9 show 16-5
16.10 show interfaces 16-6

Chapter 17: users Commands
17.1 id 17-1
17.2 pwd 17-2

Chapter 18: VNS Commands (vnsmode)
18.1 adminctr 18-1
18.1.1 flex-client-access 18-2
18.1.2 max-video-assoc 18-2
18.1.3 max-video-reassoc 18-3
18.1.4 max-voice-assoc 18-3
18.1.5 max-voice-reassoc 18-4
18.2 create 18-4
18.3 das 18-5
18.3.1 port 18-5
18.3.2 replay_interval 18-5
18.4 default-policy 18-6
18.4.1 show 18-6
18.4.2 sync 18-7

18.4.3 acfilters 18-7
18.4.3.1 create 18-8
18.4.3.2 config 18-10
18.4.3.3 delete 18-12
18.4.3.4 move 18-12
18.4.4 rateprf-in 18-13
18.4.5 rateprf-out 18-13
18.4.6 topology-name 18-14
18.4.7 ulfilterap 18-15
18.4.8 apcustom 18-15
18.4.9 apfilters 18-16
18.4.9.1 create 18-16
18.4.9.2 config 18-19
18.4.9.3 delete 18-20
18.4.9.4 move 18-21
18.5 delete 18-21
18.6 radius 18-22
18.6.1 create 18-22
18.6.2 delay-client-msg 18-23
18.6.3 delete 18-23
18.6.4 include-service-type 18-24
18.6.5 show 18-24
18.6.6 radius-mac-format 18-25
18.6.7 rename 18-26
18.6.8 strict 18-27
18.6.9 <named_RADIUS_server> 18-27
18.6.9.1 acct-port 18-27
18.6.9.2 acct-prio 18-28
18.6.9.3 acct-retries 18-28
18.6.9.4 acct-timeout 18-29
18.6.9.5 auth-port 18-29
18.6.9.6 auth-prio 18-29
18.6.9.7 auth-retries 18-30
18.6.9.8 auth-timeout 18-30
18.6.9.9 interim 18-30
18.6.9.10 ip 18-31
18.6.9.11 name 18-31
18.6.9.12 protocol 18-32
18.6.9.13 shared-secret 18-32
18.7 rateprofile 18-32
18.7.1 create 18-33
18.7.2 delete 18-33
18.7.3 show 18-34
18.8 <named-VNS> 18-34
18.8.1 auth 18-35
18.8.2 non-auth 18-35
18.8.3 name 18-36
18.8.4 pre-auth 18-37
18.8.5 restrict 18-37
18.8.6 status 18-38
18.8.7 sync 18-38
18.8.8 wlans-name 18-39
18.8.9 show 18-39

Chapter 19: wlans Commands

19.1 clients 19-1
19.1.1 client 19-2
19.1.2 descr 19-2
19.1.3 enable 19-3
19.1.4 endofday 19-3
19.1.5 export_clients 19-4
19.1.6 import_clients 19-4
19.1.7 startofday 19-5
19.2 create 19-5
19.3 delete 19-6
19.4 remote-ssid 19-6
19.5 show 19-7
19.6 <WLAN-service-name> 19-8
19.6.1 3pap 19-9
19.6.2 aplist 19-9
19.6.3 aplist-wds (WDS) 19-10
19.6.4 aplist-wds (Mesh) 19-11
19.6.5 auth 19-12
19.6.5.1 aaa-redir 19-13
19.6.5.2 auth-ap 19-13
19.6.5.3 auth-egress 19-14
19.6.5.4 auth-ingress 19-15
19.6.5.5 auth-policy 19-15
19.6.5.6 auth-ssid 19-16
19.6.5.7 auth-topology 19-17
19.6.5.8 auth-vns 19-17
19.6.5.9 captiveportal 19-18
19.6.5.9.1 add-ip-port 19-19
19.6.5.9.2 copy-cpfile 19-19
19.6.5.9.3 cp-ssl 19-19
19.6.5.9.4 custom 19-20
19.6.5.9.5 extcpip 19-20
19.6.5.9.6 extredir 19-21
19.6.5.9.7 extsecret 19-22
19.6.5.9.8 fqdn 19-22
19.6.5.9.9 guestportalacctlifetime 19-23
19.6.5.9.10 guestportalprefix 19-23
19.6.5.9.11 maxsessionlifetime 19-24
19.6.5.9.12 minpasswdlength 19-25
19.6.5.9.13 redirect 19-25
19.6.5.9.14 send-login 19-26
19.6.5.9.15 set-acct-lifetime 19-26
19.6.5.9.16 tos-override 19-27
19.6.5.10 cdr 19-27
19.6.5.11 config 19-28
19.6.5.12 config exit 19-29
19.6.5.13 interim 19-29
19.6.5.14 mac 19-30
19.6.5.15 mac-auto-authenticate 19-30
19.6.5.16 mac-allow-unauthorized 19-31
19.6.5.17 mac-roam 19-32
19.6.5.18 mode 19-32
19.6.5.19 move 19-33
19.6.5.20 nasid 19-33

19.6.5.21 nasip 19-34
19.6.5.22 password 19-35
19.6.5.23 protocol 19-35
19.6.5.24 remove 19-36
19.6.5.25 show 19-37
19.6.6 backhaul-radio 19-37
19.6.7 default-topology 19-38
19.6.8 direct-client-traffic 19-38
19.6.9 interwlan-roaming 19-39
19.6.10 name 19-39
19.6.11 priv 19-40
19.6.11.1 group-key-ps 19-40
19.6.11.2 mode 19-40
19.6.11.3 wep 19-41
19.6.11.4 wpa-broadcast-rekey 19-42
19.6.11.5 wpa-v1 19-42
19.6.11.6 wpa-v2 19-43
19.6.11.7 wpa-v2-key-mgmt 19-44
19.6.12 psk 19-44
19.6.13 qos-policy 19-45
19.6.13.1 dot11e 19-46
19.6.13.2 downlink 19-46
19.6.13.3 flex-client-access 19-47
19.6.13.4 legacy 19-47
19.6.13.5 priority-map 19-48
19.6.13.6 priority-override 19-48
19.6.13.7 priority-override-dscp 19-49
19.6.13.8 priority-override-up 19-49
19.6.13.9 turbo-voice 19-50
19.6.13.10 uapsd 19-51
19.6.13.11 uplink 19-51
19.6.13.12 wmm 19-52
19.6.13.13 video-admission-control 19-52
19.6.13.14 voice-admission-control 19-53
19.6.14 remoteable 19-54
19.6.15 rf 19-54
19.6.15.1 11h-power-reduction 19-54
19.6.15.2 11h-support 19-55
19.6.15.3 energy-save-mode 19-56
19.6.15.4 process-client-ie 19-56
19.6.15.5 show 19-56
19.6.15.6 ssid-suppress 19-57
19.6.16 show 19-57
19.6.17 ssid 19-58
19.6.18 status 19-58
19.6.19 sync 19-59
19.6.20 timeout-post 19-59
19.6.21 timeout-pre 19-60
19.6.22 timeout-session 19-61

Chapter 20: policy Commands

20.1 create 20-2
20.2 delete 20-3
20.3 enable-advance-filtering 20-3
20.4 show 20-3

20.5 <named-policy> 20-4
20.5.1 show 20-5
20.5.2 filter-status 20-5
20.5.3 name 20-6
20.5.4 sync 20-7
20.5.5 acfilters 20-8
20.5.5.1 create 20-8
20.5.5.2 config 20-11
20.5.5.3 delete 20-13
20.5.5.4 move 20-13
20.5.6 rateprf-in 20-14
20.5.7 rateprf-out 20-14
20.5.8 topology-name 20-15
20.5.9 ulfilterap 20-16
20.5.10 apcustom 20-16
20.5.11 apfilters 20-17
20.5.11.1 create 20-18
20.5.11.2 config 20-20
20.5.11.3 delete 20-22
20.5.11.4 move 20-22

Chapter 21: topology Commands

21.1 create 21-1
21.2 delete 21-2
21.3 show 21-3
21.4 <named-topology> 21-4
21.4.1 3rd-party 21-4
21.4.2 l2 21-5
21.4.2.1 multicast 21-5
21.4.2.1.1 config 21-5
21.4.2.1.2 create 21-6
21.4.2.1.3 delete 21-6
21.4.2.1.4 filter 21-7
21.4.2.1.5 move 21-7
21.4.2.1.6 show 21-7
21.4.2.2 port 21-8
21.4.2.3 show 21-8
21.4.2.4 tagged 21-9
21.4.2.5 vlanid 21-9
21.4.3 l3 21-9
21.4.3.1 ap-register 21-10
21.4.3.2 cert 21-10
21.4.3.3 copy-csr 21-12
21.4.3.4 dhcp 21-13
21.4.3.4.1 dhcp-servers 21-13
21.4.3.4.2 dls 21-14
21.4.3.4.3 dls-address 21-14
21.4.3.4.4 dns 21-15
21.4.3.4.5 domain 21-15
21.4.3.4.6 exclude 21-15
21.4.3.4.7 foreign-gateway 21-16
21.4.3.4.8 foreign-range 21-16
21.4.3.4.9 gateway 21-17
21.4.3.4.10 lease-default 21-17
21.4.3.4.11 lease-max 21-18

21.4.3.4.12 mode 21-18
21.4.3.4.13 range 21-19
21.4.3.4.14 show 21-19
21.4.3.4.15 wins 21-20
21.4.3.5 exceptions 21-21
21.4.3.5.1 config 21-21
21.4.3.5.2 create 21-23
21.4.3.5.3 delete 21-24
21.4.3.5.4 move 21-25
21.4.3.5.5 show 21-25
21.4.3.6 foreign-ip 21-26
21.4.3.7 gateway 21-26
21.4.3.8 gen-certreq 21-26
21.4.3.9 ip 21-27
21.4.3.10 mgmt 21-28
21.4.3.11 mtu 21-28
21.4.3.12 nexthop 21-28
21.4.3.13 ospf-advert 21-29
21.4.3.14 ospf-cost 21-29
21.4.3.15 show 21-30
21.4.4 l3presence 21-30
21.4.5 mode 21-31
21.4.6 name 21-31
21.4.7 show 21-32
21.4.8 strict-subnet 21-32
21.4.9 sync 21-33

Chapter 22: Location Commands (lbs)

22.1 service 22-1
22.2 server-ip 22-2
22.3 show 22-2
22.4 Related commands 22-2
22.4.1 lbs-status 22-3
22.4.2 show 22-3

Chapter 23: web Commands

23.1 guestportal-admin-timeout 23-1
23.2 timeout 23-2
23.3 showvns 23-2
23.4 show 23-3

Chapter 24: Wireless AP Diagnostics

Performing Wireless AP Diagnostics Using Telnet 24-1

About This Guide

The Command Line Interface (CLI) is used to configure the Enterasys Wireless Controller and its Wireless APs. It is accessible directly on the controller's console port, or via Secure Shell (SSH) access on the ESA or Management ports.

Who Should Use This Guide

This guide is intended for system test and development engineers who understand all components of the Enterasys Wireless Controller.

How to Use This Guide

This guide contains the following chapters:

- Chapter 1, **CLI Structure**, describes the overall context structure of the CLI.
- Chapter 2, **Common Commands**, describes commands which exist within every context level of the CLI.
- Chapter 3, **root Commands**, describes commands available from the root context of the Enterasys Wireless Controller.
- Chapter 4, **ap Commands**, describes commands which manage the basic functions of Wireless APs on a system using the Enterasys Wireless Controller.
- Chapter 5, **checkpoint Commands**, describes commands to configure Check Point software's configuration options on the Enterasys Wireless Controller.
- Chapter 6, **l2ports Commands**, describes commands enable and disable L2 ports on the Enterasys Wireless Controller.
- Chapter 7, **ip Commands**, describes commands to configure routing information.
- Chapter 8, **login Commands**, describes commands to configure the login authentication modes — local authentication and RADIUS-based authentication.
- Chapter 9, **mitigator Commands**, describes configurable options for the detection of rogue Access Points.
- Chapter 10, **mobility Commands**, describes commands to manage the exchange of client session information across a network.
- Chapter 11, **schedule_backup Commands**, describes commands to schedule data backups.
- Chapter 12, **schedule_upgrade Commands** describes commands to configure scheduling an upgrade and back up of the controller's software.
- Chapter 13, **snmp Commands**, describes commands to manage Simple Network Management Protocol (SNMP) settings for the Enterasys Wireless Controller.
- Chapter 14, **syslog Commands**, describes commands to configure System Log settings.
- Chapter 15, **time Commands**, describes commands to set system time for the Enterasys Wireless Controller, and configure network time protocol options.
- Chapter 16, **traffic_capture Commands** describes commands to manage the TCPDump.

- Chapter 17, **users Commands**, describes commands used to manage user accounts on the network.
- Chapter 18, **VNS Commands (vnsmode)**, describes commands for the setup of virtual network services (VNS) for the network.
- Chapter 19, **wlans Commands**, describes commands used to define and configure WLAN services for the network.
- Chapter 20, **policy Commands**, describes commands used to define and configure policy for the Enterasys Wireless Controller.
- Chapter 21, **topology Commands**, describes commands used to define and configure topology objects used by policy and VNS objects.
- Chapter 22, **Location Commands (lbs)**, describes commands used to configure the Enterasys Wireless Controller and Wireless APs for use with an AeroScout location based service.
- Chapter 23, **web Commands**, describes commands used to configure the web settings.
- Chapter 24, **Wireless AP Diagnostics**, describes how to configure Telnet Access features for Wireless AP diagnostics via the Enterasys Wireless Controller's graphical user interface.

Related Documentation

To access related information, see the *Enterasys Wireless Controller, Access Points and Convergence Software User Guide*. Enterasys Wireless Controller documentation is available at:

https://extranet.enterasys.com/downloads

Formatting Conventions

The following symbols are used to draw your attention to additional information:

Note: Notes identify useful information, such as reminders, tips, or other ways to perform a task.

Caution: Cautionary notes identify essential information, which if ignored can adversely affect the operation of your equipment or software.

Warning: Warning notes identify essential information, which if ignored can lead to personal injury or harm.

The following conventions are used in this guide:

Table ii-1 Conventions Used in the CLI Reference Guide

Convention	Description
Bold	This font identifies command names and key names
Italics	This font identifies references to related documentation
Courier	This font identifies text that is displayed by the computer
Bold Courier	This font identifies text input by the user
[ ]	Brackets indicate an optional parameter
< >	Angle brackets indicate a variable parameter

Table ii-1 Conventions Used in the CLI Reference Guide (continued)

Convention	Description
|	Vertical bars separate alternate parameters
( )	Round brackets create parameter groups
[< >]	Angle brackets contained in brackets indicate a required variable within an optional parameter

Note: Do not type brackets, angle brackets or vertical bars when using parameters for a command.

Keyboard Shortcuts

There are several keyboard shortcuts available to assist in navigating within the contexts of the CLI.

- To display options within a context or to complete partial entries of commands at the prompt, use **CTRL+I**, **TAB**, or the **?** key.
- To transpose mis-typed characters at the command prompt, use **CTRL+T**.
- To recall previous commands executed for the session, use the **UP ARROW**.
- To cycle forward through previously executed commands, use the **DOWN ARROW**.

Getting Help

For additional support related to the product or this document, contact Enterasys Networks using one of the following methods:

World Wide Web	www.enterasys.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000 To find the Enterasys Networks Support toll-free number in your country: www.enterasys.com/support
Email	support@enterasys.com To expedite your message, type [Wireless] in the subject line.
To send comments concerning this document to the Technical Publications Department: techpubs@enterasys.com Please include the document part number: 9034529-04 in your email message.	

Before contacting Enterasys Networks for technical support, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Enterasys Networks products in the network

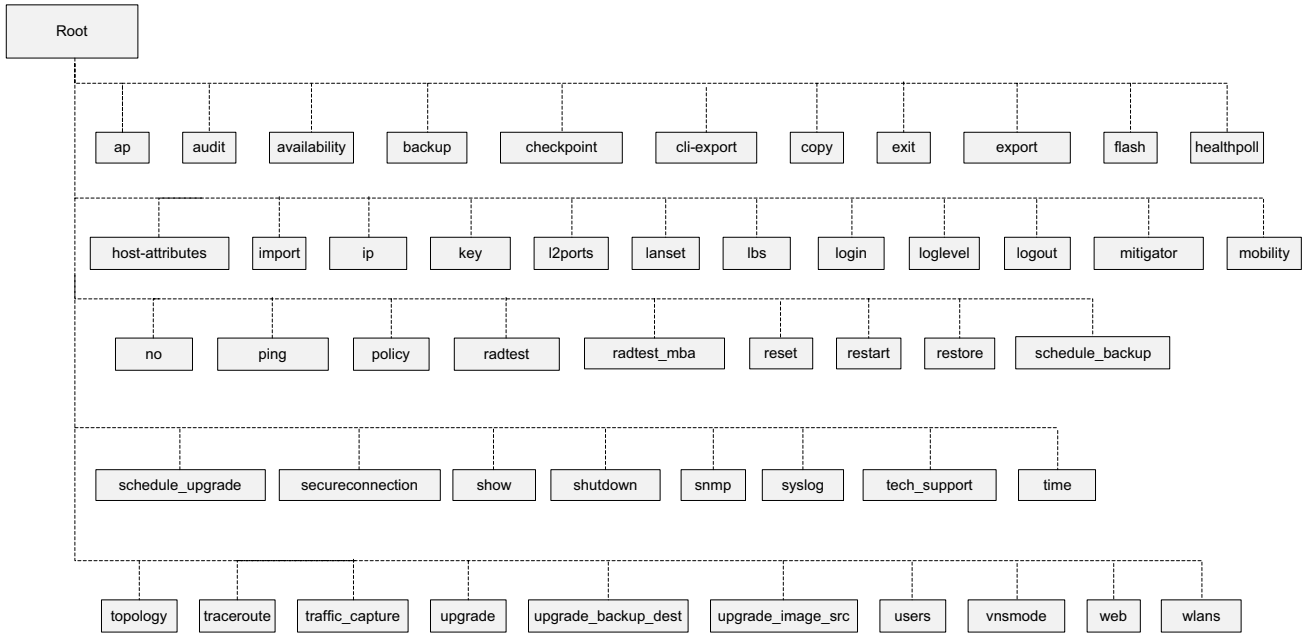
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

1

CLI Structure

The commands of the CLI are structured by context. Each context contains commands which relate to a specific function type. The following is the root context

Figure 1-1 CLI Root Structure



Account Types

Access to the CLI varies for two account types: “admin” and “user”. The admin account provides administrator access to all the contexts and features in the CLI, while the user account provides no access to contexts and command availability is limited.

The following example displays commands available in the root context for the admin account type.

```
EWC.enterasys.com# help
Available commands are:
ap                              Modify Access Point settings
audit                           Audit the Controller, delete or export the audit file
availability                    Modify availability settings
backup                          Backup Controller data to a file
checkpoint                      Modify ac checkpoint settings
```

```
copy                        Transfer files between the controller and an external server.
exit                        Return to the previous mode
export                      Backup Controller data to a file
flash                       Mount/Unmount flash drive
healthpoll                  Set healthpoll timeout
host-attributes             Configure Controller host attributes settings
import                      Restore Controller data/configuration from file
ip                          Modify controller route
key                         Modify License Keys
l2ports                     Configure Controller L2 Ports settings
lanset                      Set Ethernet link parameters
lbs                         Modify settings for AP location based service.
login
loglevel                    Set a log level
logout                      Logout
mitigator                   Modify Mitigator settings to assist in detection of rogue AP
mobility                    Modify access controller mobility settings
no                          Clear the command setting
ping                        Ping a host or gateway.
policy                      Configure Controller policy settings
radtest                     Test Radius Server connectivity, Caotive Portal and EAP
authentication
radtest_mba                 Test Radius Server connectivity and MAC-based authorization
reset                       Reset database configuration
restart                     Restart a process
restore                     Restore Controller data/configuration from file
schedule_backup             Modify backup schedule.
schedule_upgrade            Scheduled upgrade
secureconnection            Modify access controller secure connection settings
show                        Display settings
shutdown                    Used to safely halt or reboot the controller
snmp                        Configure SNMP settings
syslog                      Change syslog settings
tech_support                Collect tech support data
time                        Configure network time for the Controller
topology                    Configure Controller topology settings
traceroute                  Traceroute a host or gateway.
traffic_capture             Traffic capture on interface
upgrade                     Utility for upgrading AC software (AC), or AP software (APUP)
upgrade_backup_dest         Set ftp parameters for full disk clone backup
upgrade_image_src       Set location of upgrade image, if remote upgrade is being performed
users                       Change Controller user settings
vnsmode                     Modify Controller VNS(Virtual Network Segment) settings
web                         Modify web settings
wlans                       Configure WLAN Service settings
```

2

Common Commands

The following commands are used universally throughout the CLI shell.

2.1 apply

Use the **apply** command, after a command or a series of commands have been executed, for the configuration of the Enterasys Wireless Controller to take affect.

Syntax

```
apply
```

Parameters

None

Examples

The following example disables the DNS server configuration.

```
EWC.enterasys.com:dns# no dns 192.1.1.3
EWC.enterasys.com:dns# apply
```

Note: Unless otherwise noted, you must run the **apply** command for configuration changes to take effect.

2.2 end

Use the **end** command to return to the base context.

Syntax

```
end
```

Parameters

None

Examples

The following example returns you to the base context from the **ap:defaults** context.

```
EWC.enterasys.com:ap:defaults# end
EWC.enterasys.com#
```

2.3 exit

Use the **exit** command to return to the previous context, or to exit the shell if you are in the base context.

Syntax

```
exit
```

Parameters

None

Examples

The following example exits a context and moves up one level to the previous context.

```
EWC.enterasys.com:policy:p1# exit
EWC.enterasys.com:policy#
```

The following example exits the shell from the base context.

```
EWC# exit
```

2.4 help

Use the **help** command to display available commands in a context, or obtain usage information for a specified command.

Syntax

```
help
```

Parameters

None.

Examples

The following example displays the available commands in the **ap:defaults** context.

```
EWC.enterasys.com:ap:defaults# help
Available commands are:
11n
4102                            Modify 4102 ap defaults settings
apply                           Commit AP default changes.
assign                          Modify AP default VNS assignment settings
dualband                        Modify dualband ap defaults settings
end
exit
learnac                         Enable/disable learn on the AP.
logout
no                              Clear the command setting
show                            Display settings
std                             Modify standard ap defaults settings
```

2.5 logout

Use the **logout** command to exit the shell immediately.

Syntax

```
logout
```

Parameters

None

Examples

The following example exits the shell.

```
EWC.enterasys.com:interface:eth0# logout
```

2.6 no

Use the **no** option to disable a function of a command. Use the command's syntax without the **no** form to enable it. The **no** option can also be used to delete settings or files when used with certain commands.

Note: Not all commands within the CLI include a **no** option.

Syntax

```
no
```

Parameters

None

Examples

The following example configures and displays a gateway IP address, then disables it with the **no** command and displays the change.

```
EWC.enterasys.com:interface:eth0# gateway 192.176.3.4
EWC.enterasys.com:interface:eth0# show gateway
gateway 192.176.3.4
EWC.enterasys.com:interface:eth0# no gateway
EWC.enterasys.com:interface:eth0# show gateway
no gateway
```

2.7 show

Use the **show** command to display the current configuration within a context.

Syntax

```
show
```

Parameters

None

Examples

The following example displays the DNS configuration.

```
EWC.enterasys.com:dns# show
dns 1 192.1.1.3
dns 2 192.1.2.3
dns 3 192.1.3.3
```

3

root Commands

The root context of the CLI displays available commands relating to the Enterasys Wireless Controller's configuration, as well as available sub-contexts.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

This chapter documents root context commands not associated with features documented in other chapters. See Table 3-1 for a listing and description of root commands documented outside of this chapter.

Table 3-1 Root Commands Documented in Feature Chapters

Command	Description
ap	The **ap** command moves you to the ap context of the CLI, providing access to commands required to manage the basic functions of the Wireless APs on the system. See Chapter 4, **ap Commands**.
checkpoint	The **checkpoint** command moves you to the checkpoint context of the CLI, providing access to commands which enable and configure Check Point event logging options for the Enterasys Wireless Controller. See Chapter 5, **checkpoint Commands**.
exit	The **exit** command returns to the previous context or exits the shell if you are in the base context. See "2.3, exit" on page 2-2.
ip	The **ip** command moves you to the ip context of the CLI, providing access to commands for the configuration of routing information. See Chapter 7, **ip Commands**.
l2ports	The **l2ports** command moves you to the l2ports context of the CLI, providing access to commands for the enabling and disabling of ports. See Chapter 6, **l2ports Commands**.
login	The **login** command moves you to the login context of the CLI, providing access to commands for the configuration of the login authentication modes . See Chapter 8, **login Commands**.
logout	The **logout** command exits the shell immediately. See "2.5, logout" on page 2-3.
mitigator	The **mitigator** command moves you to the mitigator context of the CLI, providing commnads that assist in the detection of rogue Access Points. See Chapter 9, **mitigator Commands**.

Table 3-1 Root Commands Documented in Feature Chapters (continued)

Command	Description
mobility	The **mobility** command moves you to the mobility context of the CLI, providing commands that configure the sharing and exchanging of client session information, which enables a wireless device to roam between Wireless APs on different Enterasys Wireless Controllers without service interruption. See Chapter 10, **mobility Commands**.
policy	The **policy** command moves you to the policy context of the CLI, providing commands for the defining and configuring of policy for the Enterasys Wireless Controller. See Chapter 20, **policy Commands**.
schedule_backup	The **schedule_backup** command moves you to the schedule_backup context of the CLI, providing commands for backup scheduling of software configurations, CDR, log, audit, and rogue AP reports and databases. See Chapter 11, **schedule_backup Commands**.
schedule_upgrade	The **schedule_upgrade** command moves you to the schedule_upgrade context of the CLI, providing commands for scheduling an upgrade and back up of the controller's software. See Chapter 12, **schedule_upgrade Commands**.
snmp	The **snmp** command moves you to the snmp context of the CLI, providing for the management of SNMP settings for the Enterasys Wireless Controller. See Chapter 13, **snmp Commands**.
syslog	The **syslog** command moves you to the syslog context of the CLI, providing for the configuration of system log settings on the Enterasys Wireless Controller. See Chapter 14, **syslog Commands**.
time	The **time** command moves you to the time context of the CLI, providing for synchronization network elements on the Enterasys Wireless Controller to a universal clock using the Enterasys Wireless Controller's own system time or the Network Time Protocol. See Chapter 15, **time Commands**.
topology	The **topology** command moves you to the topology context of the CLI, providing for defining and configuration of topology objects used by policy and VNS objects. See Chapter 21, **topology Commands**.
traffic_capture	The **traffic_capture** command moves you to the traffic_capture context of the CLI, providing for the management of the TCPDump. See Chapter 16, **traffic_capture Commands**.
users	The **users** command moves you to the users context of the CLI, providing for commands used to create and manage user accounts on the network. Chapter 17, **users Commands**.
vnsmode	The **vnsmode** command moves you to the vnsmode context of the CLI, providing for commands used to define and configure Virtual Network Services (VNS) for the network. See Chapter 18, **VNS Commands (vnsmode)**.
web	The **web** command moves you to the web context of the CLI, providing for commands to configure the web settings. See Chapter 23, **web Commands**.
wlans	The **wlans** command moves you to the wlans context of the CLI, providing for commands used to define and configure WLAN services for the network. See Chapter 19, **wlans Commands**.

3.1 audit

Use the **audit** command to delete audit information or export it to a temporary file directory on the Enterasys Wireless Controller.

Syntax

```
audit (delete|export)
```

Parameters

delete	Indicates that audit information will be deleted
export	Indicates that audit information will be exported

Examples

The following example deletes audit information from the Enterasys Wireless Controller

```
EWC.enterasys.com# audit delete
```

The following example exports the audit information into a temporary file directory

```
EWC.enterasys.com# audit export
Exported audit file to /tmp/reports/10870877310LogMsg
```

3.2 availability

Switch to the **availability** context from the root context to access the following commands on the Enterasys Wireless Controller.

Note: The **availability** context was introduced with V6R1. The following commands from the **ap:registration** context ("4.8, registration" on page 4-131) have been moved to the **availability** command context: pair, pairip, pairrole, fast_failover, and link_timeout.

3.2.1 pair

Use the **pair** command to set up two Enterasys Wireless Controllers as a pair. Use the **no** form of the command to set up Enterasys Wireless Controllers in stand-alone mode.

Syntax

```
pair <A.B.C.D> (primary|secondary)
```

Parameters

<A.B.C.D>	Specifies the IP address of the backup Enterasys Wireless Controller.
(primary|secondary)	Specifies if the Enterasys Wireless Controller is the primary or secondary controller in the pair.

Examples

```
EWC.enterasys.com:availability# pair 123.321.24.54 primary
```

3.2.2 pairip

Use the **pairip** command to specify the backup of the Enterasys Wireless Controller's IP address.

Syntax

```
pairip <IP Address>
```

Parameters

<IP Address>	Specifies the IP address of the backup controller

Examples

The following example sets an IP address for the backup Enterasys Wireless Controller

```
EWC.enterasys.com:availability# pairip 123.321.24.54
```

3.2.3 pairrole

Use the **pairrole** command to designate the Enterasys Wireless Controller as the primary connection point for availability Link Exchange or as the secondary point.

Note: When an Enterasys Wireless Controller is set as the secondary connection point, Wireless AP registration requests will be set to pending until the other Enterasys Wireless Controller is set up as the primary connection point.

Syntax

```
pairrole (primary|secondary)
```

Parameters

primary	Assigns the primary connection point role
secondary	Assigns the secondary connection point role

Examples

The following example sets the current Enterasys Wireless Controller to be the primary connection point

```
EWC.enterasys.com:availability# pairrole primary
```

3.2.4 fast_failover

Use the **fast_failover** command to enable fast failover of the Wireless APs to the secondary controller in 'availability' mode. Use the **no** form of the command to disable the fast failover feature.

Syntax

```
fast_failover
no fast_failover
```

Parameters

None

Examples

```
EWC.enterasys.com:availability# fast_failover
```

3.2.5 link_timeout

Use the **link_timeout** command to specify the time period in which the link failure between the Wireless APs and the primary controller in 'availability' mode would be detected.

Syntax

```
link_timeout <seconds>
```

Parameters

<seconds>	Specifies time period in seconds before link failure is detected

Examples

The following example sets the time for link failure detection to 10 seconds

```
EWC.enterasys.com:availability# link_timeout 10
```

Note: The time for the link failure is in seconds. You can specify the time for link failure detection between the range of 2 to 30 seconds.

3.2.6 sync-config

Use the **sync-config** command to enable or disable synchronization of the configuration elements.

Syntax

```
sync-config enable | disable
```

Parameters

enable	Enable synchronization of the configuration elements.
disable	Disable synchronization of the configuration elements.

Examples

The following example enables the synchronization of the configuration elements.

```
EWC.enterasys.com:availability# sync-config enable
```

3.2.7 sync-mu

Use the **sync-mu** command to enable or disable synchronization of MU accounts.

Syntax

```
[no] sync-mu
```

Parameters

None.

Examples

The following example enables the synchronization of the MU accounts.

```
EWC.enterasys.com:availability# sync-mu
```

3.3 backup

Use the **backup** command to save Enterasys Wireless Controller data to a file.

Syntax

```
backup (configuration|cdrs|all|logs|audit|rogue)
```

Parameters

`configuration`	Creates a backup of the configuration data
`cdrs`	Creates a backup of the Call Detail Records data
`all`	Creates a backup of the configuration, logs, audit, rogue and Call Detail Records data
`logs`	Creates a backup of the logs
`audit`	Creates a backup of the audit data
`rogue`	Creates a backup of the rogue data

Examples

The following example creates a backup of the Call Detail Records data

```
EWC.enterasys.com# backup cdrs
Filename (lab-91-f.16082010.102250):
Comment:
Please wait...
Creating lab-91-f.16082010.102250...
Backup/Export complete.

EWC.enterasys.com#
```

3.4 copy

Use the **copy** command to transfer files between the Enterasys Wireless Controller and an external server.

Note: Available filenames and platform information can be retrieved by invoking the respective **show** commands. For more information, see "3.21, show" on page 3-23.

Syntax

```
copy ap_certreq <server> <user> <dir> <file>
copy apup <server> <user> <dir> <file> <platform>
copy backup <server> <user> <dir> <file> [<scp> <scp password>]
copy cdrs <server> <user> <dir> <cdr_dir/file>
copy export <server> <user> <dir> <file> [<scp> <scp password>]
copy import <server> <user> <dir> <file> [<scp> <scp password>]
copy restore <server> <user> <dir> <file> [<scp> <scp password>]
copy sensor <tftp_server> <dir> <file> (AP26xx | AP36xx)
copy tcpdump <server> <user> <dir> <file>|<#file>
copy tech_support <server> <user> <dir> <file> [<scp> <scp password>]
copy upgrade <server> <user> <dir> <file> [flash]
copy upgrade_history <server> <user> <dir>
```

Parameters

<server>	Specifies the IP address of the FTP or SCP server
<user>	Specifies the user name of an account on the FTP or SCP server
<dir>	Specifies the name of a directory on the FTP or SCP server
<file>	Specifies the name of a file on the Enterasys Wireless Controller
<platform>	Specifies the platform of the Wireless AP
<cdr_dir/file>	Specifies the location of a file on the Enterasys Wireless Controller
<#file>	The sequence in which the files are listed in the TCPDump capture file list. For more information, see "16.6, list" on page 16-4.
[scp]	Sets the file transfer protocol to SCP rather than the default setting of FTP
<scp password>	The scp password to use with scp for the ssh connection
[flash]	This option is available only when a flash card is plugged in. This is supported on all platforms except the CRBT8210.

Examples

The following example copies the certificate request (.csr) file for a Wireless AP.

```
EWC.enterasys.com# copy ap_certreq 192.168.1.131 jdoe /jdoe/OrlandoAP.csr
```

The following command copies the Call Detail Records from the Enterasys Wireless Controller onto the specified server location.

```
EWC.enterasys.com# copy cdrs 192.168.4.181 administrator /20070906200754.dat
```

```
Please input password:
Attempting to upload file...
SUCCESS: Upload completed.
```

The following command copies an upgrade image for the W788 platform from a server to the Enterasys Wireless Controller.

```
EWC.enterasys.com# copy apup 192.168.16.21 test new/ap/ W788-07.41.03.0003.img
W788
Please input password:
Attempting to download file using ftp ...
SUCCESS: FTP Download completed.
EWC.enterasys.com#
```

The following command copies a restore file from a specific server to the Enterasys Wireless Controller.

```
EWC.enterasys.com# copy EWC.enterasys.com: 192.168.1.131 jdoe /jdoe/restore
bc.zip
```

The following command copies the Enterasys Wireless Controller's upgrade image from a specific server location onto the Enterasys Wireless Controller.

```
EWC.enterasys.com# copy upgrade 192.168.16.21 test new/ac/rpm/build07.41.03.0003
AC-MV-07.41.03.0003-1.gps
Please input password:
Attempting to download file using ftp ...
SUCCESS: FTP Download completed.
EWC.enterasys.com#
```

The following example copies the upgrade file to the flash card, mounted on the Enterasys Wireless Controller, from a specific server.

```
EWC.enterasys.com# copy upgrade 192.168.16.21 test new/ac/rpm/build07.41.03.0003
AC-MV-07.41.03.0003-1.gps flash
Please input password:
Attempting to download file using ftp ...
SUCCESS: FTP Download completed.
EWC.enterasys.com#
```

The following example copies the TCPDump file to the FTP server.

```
EWC.enterasys.com# copy tcpdump 192.168.4.10 mnj /TCPDump/April_2008
mgmt_traffic_capture.cap 1
```

3.5 host-attributes

Switch to the **host-attributes** context from the root context to configure host attributes on the Enterasys Wireless Controller.

Syntax

```
host-attributes
```

Parameters

None

Examples

```
EWC.enterasys.com# host-attributes
EWC.enterasys.com:host-attributes#
```

3.5.1 hostname

Use the **hostname** command to configure a hostname for the controller.

Syntax

```
hostname <name> | none
```

Parameters

<name>	Specifies the hostname of the controller.
none	Removes the configured hostname.

Examples

The following example specifies that the host name of the controller should be EWC123.

```
EWC.enterasys.com:host-attributes# hostname EWC123
EWC.enterasys.com:host-attributes# apply
```

Note: After you have run the **hostname** command, you must run the **apply** command to implement the changes.

3.5.2 domain

Use the **domain** command to configure the domain name for the controller.

Syntax

```
domain <domain name> | none
```

Parameters

<domain name>	Specifies the domain name of the controller.
none	Removes the configured domain name.

Examples

The following example specifies that the domain name of the controller should be enterasys.com.

```
EWC.enterasys.com:host-attributes# domaain enterasys.com
EWC.enterasys.com:host-attributes# apply
```

Note: After you have run the **domain** command, you must run the **apply** command to implement the changes.

3.5.3 dns

Use the **dns** command at the **host-attributes** context to move into DNS server configuration context.

Syntax

```
dns
```

Parameters

None

Examples

```
EWC.enterasys.com:host-attributes# dns
EWC.enterasys.com:host-attributes:dns#
```

3.5.3.1 dns

Use the **dns** command in the **dns** context to configure DNS servers for the controller. You can configure up to three DNS servers to resolve RADIUS server host names to their corresponding IP addresses. Use the **no** form of the command to remove a DNS server configuration.

Syntax

```
dns <[1-3]> <ip address>
no dns <[1-3]> <ip address>
```

Parameters

`<[1-3]>`	Specifies the position of the DNS server in the DNS servers list.
`<ip address>`	Specifies the IP address of the DNS server.

Note: After you have run the **dns** command, you must run the **apply** command to implement the changes.

Examples

The following example defines a DNS server, with a 192.1.1.3 IP address, as the first DNS server.

```
EWC.enterasys.com:host-attributes:dns# dns 1 192.1.1.3
```

3.5.3.2 move

Use the **move** command in the **dns** context to reposition DNS servers in the DNS server list.

Syntax

```
move <orig_index> <new_index>
```

Parameters

`<orig_index>`	Specifies the current position of the DNS server that you want to reposition.

<new_index>	Specifies the new position of the DNS server that you want to reposition.

Note: After you have run the **move** command, you must run the **apply** command to implement the changes.

Examples

The following example displays the current DNS server configuration.

```
EWC.enterasys.com:host-attributes:dns# show
dns 1 192.1.1.3
dns 2 192.1.2.3
dns 3 192.1.3.3
```

To move the DNS sever 192.1.3.3 into the first position on the DNS servers list, use the following command:

```
host-attributes:dns# move 3 1
```

The following displays the results of the previous **move** command:

```
EWC.enterasys.com:host-attributes:dns# show
dns 1 192.1.3.3
dns 2 192.1.1.3
dns 3 192.1.2.3
```

3.6 export

Use the **export** command to export the controller's configuration, CDRs, logs audit information and rogue data or all of them in *a .zip* file.

Syntax

```
export (configuration|cdrs|all|logs|audit|rogue)
```

Parameters

configuration	Exports the controller's configuration
cdrs	Exports the controller's CDRs
all	Exports all of the following: controller's configuration, CDRs, logs, audit information and rogue data
logs	Exports the controller's logs
audit	Exports the controller's audit information
rogue	Exports the controller's rogue data

Examples

The following command exports the controller's existing configuration in a .zip file.

```
EWC.enterasys.com# export configuration
```

```
Filename (lab-91-f.16082010.110525):
Comment:
Please wait...
CLI Export start: Mon Aug 16 11:05:33 2010
CLI Export end: Mon Aug 16 11:05:37 2010
Creating lab-91-f.16082010.110525...
Backup/Export complete.
```

The following example exports the controller's CDRs in a .zip file.

```
EWC.enterasys.com# export cdrs
Filename (lab-91-f.16082010.110544):
Comment:
Please wait...
Creating lab-91-f.16082010.110544...
Backup/Export complete.
```

The following example exports the controller's logs in a .zip file.

```
EWC.enterasys.com# export logs
Filename (lab-91-f.16082010.110548):
Comment:
Please wait...
Creating lab-91-f.16082010.110548...
Backup/Export complete.
```

The following example exports the controller's audit information in a .zip file.

```
EWC.enterasys.com# export audit
Filename (lab-91-f.16082010.110554):
Comment:
Please wait...
Creating lab-91-f.16082010.110554...
Backup/Export complete.
```

The following example exports the controller's rogue data in a .zip file.

```
EWC.enterasys.com# export rogue
Filename (lab-91-f.16082010.110641):
Comment:
Please wait...
CLI Export start: Mon Aug 16 11:06:47 2010
CLI Export end: Mon Aug 16 11:06:50 2010
Creating lab-91-f.16082010.110641...
Backup/Export complete.
```

The following example exports all of the following: Configuration, CDRs, logs, audit information, and rogue data.

```
EWC.enterasys.com# export all
Filename (lab-91-f.16082010.110654):
Comment:
Please wait...
```

```
CLI Export start: Mon Aug 16 11:06:59 2010
CLI Export end: Mon Aug 16 11:07:03 2010
Creating lab-91-f.16082010.110654...
Backup/Export complete.

EWC.enterasys.com#
```

Note: During the export process, the *.zip* file containing the controller's data is zipped. The exported file displays *.zip* extension.

Note: If you want to upload the controller's data to the FTP server, you must use the `copy backup` command. For more information, see "3.4, copy" on page 3-7.

3.7 flash

Use the **flash** command to mount or dismount the flash card on the Enterasys Wireless Controller.

Syntax

```
flash <mount|unmount>
```

Parameters

<mount>	Specifies to mount the flash card
<unmount>	Specifies to dismount the flash card

Examples

The following example mounts the flash card on the Enterasys Wireless Controller.

```
EWC.enterasys.com# flash mount
```

The following example dismounts the flash card from the Enterasys Wireless Controller.

```
EWC.enterasys.com# flash unmount
```

3.8 no flash

Use the **no flash** command to delete files on a flash card. The **no flash** command is under the root context.

Note: This command is not accessible on platforms that do no support flash devices.

Syntax

```
no flash <file name>
```

Examples

The following example deletes the files from the flash card.

```
EWC.enterasys.com# no flash lab-91-f.16082010.110525
```

```
Successfully deleted file lab-91-f.16082010.110525 from flash
```

3.9 healthpoll

Use the **healthpoll** command to enable or disable the poll timer.

Syntax

```
healthpoll <enable|disable>
```

Parameters

enable	Enables the poll timer
disable	Disables the poll timer

Examples

The following command enables the poll timer

```
EWC.enterasys.com# healthpoll enable
EWC.enterasys.com# show healthpoll
healthpoll enable
```

3.10 import

Use the **import** command to import the controller's configuration, CDRs, logs, audit information, and rogue data from a text file that was earlier exported from a previous platform or an old software release.

Syntax

```
[no] import <filename|number>
```

Parameters

file name	The name of the *.zip* or *.cli* file that contains the controller's configuration, rogue data, or both.
number	The order number (sequence number) in which the *.zip* or *.cli* file is displayed on the CLI interface.

Examples

The following command imports the controller's configuration, CDRS, logs, audit information and rogue data from a 'zipped' *.zip* file that was exported from the previous platform or from the older software.

```
EWC.enterasys.com# import lab-213-g.11042008.141154.zip
```

Note: If you want to import the controller's data from a remote FTP server, you must use the **copy restore** command. For more information, see "3.4, copy" on page 3-7.

3.11 key

Use the **key** command to configure license key information for the Enterasys Wireless Controller.

Syntax

```
key
```

Parameters

None

Examples

```
EWC.enterasys.com# key
```

3.11.1 activate

Use the **activate** command to apply a license key on the Enterasys Wireless Controller. The **activate** command is accessible from the **key** context of the CLI.

Syntax

```
activate <activation-key>
```

Parameters

<activation-key>	Specifies the license key to be applied on the Enterasys Wireless Controller. The license key format is: AAAAAAA-11111111-11111111-11111111-11111111

Examples

The following example applies a license key on the Enterasys Wireless Controller.

```
EWC.enterasys.com:key# activate ABCDEFG-12345678-22345678-32345678-42345678
```

3.11.2 ecap

Use the **ecap** command to apply a capacity enhancement license key on the Enterasys Wireless Controller. The **ecap** command is accessible from the **key** context of the CLI.

Syntax

```
ecap <ecap-key>
```

Parameters

<ecap-key>>	Specifies the capacity enhancement license key to be applied on the Enterasys Wireless Controller. The capacity enhancement license key format is: CAPCTL-11111111-11111111-11111111-11111111 For the C20/C20N platforms, the capacity enhancement license key format is: CAPC20-11111111-11111111-11111111-11111111

Examples

The following example applies a capacity enhancement license key on the Enterasys Wireless Controller.

```
EWC.enterasys.com:key# ecap CAPCTL-12345678-22345678-32345678-42345678
```

3.11.3 extcp

Use the **extcp** command to apply an external captive portal license key on the Enterasys Wireless Controller. The **extcp** command is accessible from the **key** context of the CLI.

Syntax

```
extcp <extcp-key>
```

Parameters

<extcp-key>	Specifies the external captive portal license key to be applied on the Enterasys Wireless Controller. The external captive portal license key format is: EXTCP-11111111-11111111-11111111-11111111

Examples

The following example applies an external captive portal license key on the Enterasys Wireless Controller.

```
EWC.enterasys.com:key# extcp EXTCP-12345678-22345678-32345678-42345678
```

3.12 lanset

Use the **lanset** command to define the port speed — the data transmission rate of an output/input channel. The **lanset** command is available at the root context of the admin account type.

Syntax

```
lanset <lanN|admin> <autoneg_off|autoneg_on> <10|100|1000|any> [full|half|both]
```

Parameters

lan*N*	Specifies the data port. *N* can range from 1 to 4, depending on the controller model.
admin	Admin Port
autoneg_on	Allows PHY (Physical Layer) to auto-negotiate the port speed and the duplex mode
autoneg_off	Disallows PHY to auto-negotiate the port speed and the duplex mode
10	Sets the port speed to 10 Mbps
100	Sets the port speed to 100 Mbps
1000	Sets the port speed to 1000 Mbps

any	Allows the PHY to negotiate the port speed from any of the three options — 10, 100 or 1000 Mbps — and the duplex mode from any of the two option options — half-duplex or full-duplex
full	Allows the PHY to operate in full duplex mode
half	Allows the PHY to operate in half-duplex mode
both	Allows the PHY to auto-negotiate either half-duplex mode or the full-duplex mode

Examples for an Admin Port

The following example sets the port speed to 100 Mbps, full duplex mode, and disables auto-negotiation for the admin port.

```
EWC.enterasys.com# lanset admin autoneg_off 100 full
```

Caution: In the case of an Admin Port, the **lanset** command does not support a port speed of 1000 Mbps with auto-negotiation off (**autoneg_off**). However, with auto-negotiation on (**autoneg_on**), the **lanset** command allows the PHY to negotiate a port speed of 1000 Mbps in full-duplex mode.

The following example enables auto-negotiation for any port speed and either duplex mode for the admin port..

```
EWC.enterasys.com# lanset admin autoneg_on any
```

Examples for Data Ports

The following example disables auto-negotiation and sets the port speed to 100 Mbps in full duplex mode for data port 1.

```
EWC.enterasys.com# lanset lan1 autoneg_off 100 full
```

Caution: In the case of Data Ports, the **lanset** command does not support a port speed of 1000 Mbps with auto-negotiation disabled. The **lanset** command supports a port speed of 1000 Mbps with auto-negotiation enabled only in full-duplex mode.

Note: In the case of Data Ports, the **lanset** command supports multiple options with auto-negotiation enabled.

The following example enables auto-negotiation for data port 1 and allows setting the port speed from the following options: 1000 Mbps in full-duplex mode, 10 Mbps in half-duplex mode, and 100 Mbps in both the modes i.e., half-duplex and full-duplex.

```
EWC.enterasys.com# lanset lan1 autoneg_on 1000 full 10 half 100 both
```

3.13 loglevel

Use the **loglevel** command to set the log level for the Enterasys Wireless Controller or the Wireless AP.

Syntax

```
loglevel ac (1|2|3|4) | ap (1|2|3|4)
```

Parameters

ac	Sets the log level of the Enterasys Wireless Controller
ap	Sets the log level of the Wireless AP
1	Indicates Critical severity level
2	Indicates Major severity level
3	Indicates Minor severity level
4	Indicates Informational severity level

Examples

The following example sets the Enterasys Wireless Controller's log level to Minor

```
EWC.enterasys.com# loglevel ac 3
Successfully set ac log level to Minor (3)
```

3.14 ping

Use the **ping** command to ping an IP address. As of V7.0, the ping command accepts an optional parameter that specifies the source ip address to be used by the command. If this optional source is provided, ping uses the IP address of the specified interface as the source IP address.

Syntax

```
ping [source-interface (name <name>) | (number <id>)] <ip address>
```

Parameters

source-interface (name <name>) | (number <id>)	Specifies the address of the source interface you want to send pings from, either by interface name or ID.
<IP Address>	Specifies the IP address you want to ping

Usage

You can identify the source IP using its interface name or, for short, the identifier returned by the **show topology l3** command. Interface name is the name of any topology with L3 configuration (Physical, Admin, B@AC or Routed).

Examples

The following example pings an IP address

```
EWC.enterasys.com# ping 192.168.1.32
PING 192.168.1.32 (192.168.1.32) from 192.168.1.38 : 56(84) bytes of data.
64 bytes from 192.168.1.32: icmp_seq=1 ttl=64 time=0.423 ms
64 bytes from 192.168.1.32: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 192.168.1.32: icmp_seq=3 ttl=64 time=0.204 ms

--- 192.168.1.32 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2013ms
```

```
rtt min/avg/max/mdev = 0.204/0.281/0.423/0.101 ms
```

The following example first uses the **show topology l3** command to obtain interface names for use with ping as source addresses. Then, the following command pings an IP address using the IP address of interface name "esa1" (as determined with the the **show topology l3** command) as the source address.

```
EWC.enterasys.com# show topology l3

Name                                Mode                L3:IP

1:Admin                             admin               192.168.4.37
2:esa0                              physical            10.0.0.1
3:esa1                              physical            10.0.1.1
4:Enterasys-37Topology              b@ac                10.10.1.1
EWC.enterasys.com# ping source-interface name esa1 192.168.4.37
PING 192.168.4.37 (192.168.4.37) from 10.0.1.1 : 56(84) bytes of data.
64 bytes from 192.168.4.37: icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from 192.168.4.37: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 192.168.4.37: icmp_seq=3 ttl=64 time=0.039 ms

--- 192.168.4.37 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.037/0.039/0.042/0.005 ms
```

3.15 radtest

Use the **radtest** command to test the RADIUS server's connectivity and configuration.

Syntax

```
radtest <vns_name> <username> <password> [tracing]
radtest <vns_name> <username> [tracing]
```

Parameters

<vns_name>	Specifies the VNS server
<username>	Specifies a username
<password>	Specifies a password
tracing	Specifies that tracing will be used

Examples

The following example tests the radius server on CNL-7-CP

```
EWC.enterasys.com# radtest CNL-7-CP sales abc123 tracing
Sending Captive portal authentication request to Radius Server for user sales,
with password abc123, on vns_name CNL-7-CP.
```

```
Please wait while all configured Radius Servers on this VNS are attempted as needed
...
Turned tracing on for Radius Client.
TRACE: Radius Request: CP: Server:192.0.1.202 Port:1812 Authtype:2 Username:sales
Retries:0
Test Completed.
```

3.16 radtest_mba

Use the **radtest_mba** command to test RADIUS servers used by the Enterasys Wireless Controller for Mac-based authorization.

Syntax

```
radtest_mba <vns_name> <MAC Address> <ap_bss_mac_addr> <ap_eth_mac_addr>
[tracing]
```

Parameters

<vns_name>	Specifies the VNS server
<MAC Address>	Specifies a MAC address
<ap_bss_mac_addr>	Specifies the Wireless AP's Basic Service Set Identifier (BSSID)
<ap_eth_mac_addr>	Specifies the Wireless AP's ethernet MAC address
tracing	Specifies that tracing will be used

Examples

The following example tests the RADIUS server on CNL-206-CPWEP

```
EWC.enterasys.com# radtest_mba CNL-206-CPWEP 00:0E:35:CA:D1:96
Sending MAC-based authorization request to Radius Server for mac_str
00:0E:35:CA:D1:96 on vns_name CNL-206-CPWEP with bss_mac DE:AD:DE:AD:DE:AD and
eth_mac DE:AD:DE:AD:DE:AD.
Please wait while all configured Radius Servers on this VNS are attempted as needed
...
Test Completed.
```

3.17 reset

Use the **reset** command to reset configuration settings on the Enterasys Wireless Controller to their factory defaults.

Note: The database and factory options for the reset command have been superceded by the options described here beginning with the V6R1 release.

Syntax

```
reset [license] [mgmt]
```

Parameters

license	Removes the installed license.
mgmt	Resets the management port configuration.

Examples

1. The following example resets all configuration settings on the Enterasys Wireless Controller except for the management port configuration. You are prompted to confirm if you want to continue to reset the Enterasys Wireless Controller.

```
EWC.enterasys.com# reset
WARNING: Resetting will clear all configuration except for the management port
configuration. It will disconnect any clients currently using the system.
Following the reset, the system will be rebooted.
Do you wish to continue? (y/n)
```

2. The following example resets all configuration settings on the Enterasys Wireless Controller including the management port configuration. You are prompted to confirm if you want to continue to reset the Enterasys Wireless Controller.

```
EWC.enterasys.com# reset mgmt
WARNING: Resetting management will clear all configuration including the
management port configuration. It will disconnect any clients currently using the
system. Following the reset, the system will be rebooted.
Do you wish to continue? (y/n)
```

3. The following example removes installed licenses and resets all configuration settings on the Enterasys Wireless Controller except for the management port configuration. You are prompted to confirm if you want to continue to reset the Enterasys Wireless Controller.

```
EWC.enterasys.com# reset license
WARNING: Resetting the license will clear all configuration and permanently delete
any installed licenses. It will disconnect any clients currently using the system.
Following the reset, the system will be rebooted.
Activation key string : XXXXXXX-XXXXXXX-XXXXXXX-XXXXXXX-XXXXXXX
External Captive Portal Option Key:
Capacity Enhancement Option Keys:
Do you wish to continue? (y/n)
```

4. The following example removes installed licenses and resets all configuration settings on the Enterasys Wireless Controller including the management port configuration. You are prompted to confirm if you want to continue to reset the Enterasys Wireless Controller.

```
EWC.enterasys.com# reset license mgmt
WARNING: Resetting the license and management will clear all configuration and
permanently delete any installed licenses. It will disconnect any clients
currently using the system. Following the reset, the system will be rebooted.
Activation key string : XXXXXXX-XXXXXXX-XXXXXXX-XXXXXXX-XXXXXXX
External Captive Portal Option Key:
Capacity Enhancement Option Keys:
Do you wish to continue? (y/n)
```

3.18 restart

Use the **restart** command to restart individual processes on the Enterasys Wireless Controller.

Note: Use the show system_state process command to list the current processes on the Active Controller. For more information, see "3.21.39, show system_state" on page 3-56.

Syntax

```
restart <process_id> | <process_name>
```

Parameters

<process_id>	Specifies the process name
<process_name>	Specifies the index number of the process

Examples

The following command restarts the LLC Handler process by referring to its index number

```
EWC.enterasys.com# restart 1094
LLC Handler process being restarted.
```

3.19 restore

Use the **restore** command to restore data and configurations on the Enterasys Wireless Controller.

Note: Use **show restore** to view a list of available files that can be restored on the Enterasys Wireless Controller. For more information, see "3.21.32, show restore" on page 3-50.

Syntax

```
restore <filename>|<number>
```

Parameters

<filename>	Specifies the name of the restore file
<number>	Specifies the index number of the restore file. You can use the **show restore** command or **show backup** command to find the restore file's index number.

Examples

The following example restores the second file from a restore list onto the Enterasys Wireless Controller

```
EWC.enterasys.com# restore 2
WARNING: after restoring/importing, system will be rebooted
Do you wish to continue? (y/n) y
```

3.20 secureconnection

Use the **secureconnection** command to configure the shared secret between a Enterasys Wireless Controller and NetSight Wireless Manager.

3.20.1 secret

Use the **secret** command to configure a shared secret for a Enterasys Wireless Controller and NetSight Wireless Manager. Use the **no** command to disable the shared secret. The secret command is available from the **secureconnection** context of the CLI.

Syntax

```
secret <A.B.C.D> <secret_string>
no secret
```

Parameters

<A.B.C.D>	Specifies the NetSight Wireless Manager's IP address
<secret_string>	Specifies the shared secret string.

Examples

```
EWC.enterasys.com:secureconnection# secret 200.200.200.200 1234567890123456
```

3.21 show

The CLI is equipped with **show** commands, which are used to display properties and configurations of component features on the Enterasys Wireless Controller. The **show** commands are accessible from the root context of the CLI.

3.21.1 show ac version

Use the **show ac version** command to display the software version, software build, and hardware platform versions of the Enterasys Wireless Controller.

Syntax

```
show ac version
```

Parameters

None

Examples

The following example displays the software version, software build and hardware platform version of the Enterasys Wireless Controller

```
EWC.enterasys.com# show ac version
Software version: 7.41
Software build: 07.41.01.0118T
Product Name: C2400 Enterprise
```

3.21.2 show active-user

Use ths command to display the currently logged in user.

Syntax

```
show active-user
```

Parameters

None.

Examples

```
EWC.enterasys.com# show active-user
User: admin
```

3.21.3 show ap

Use the **show ap** command to show the configuration information of Wireless APs connected to the Enterasys Wireless Controller.

Syntax

```
show ap [access | registration | version | load-groups | defaults [config |
standard | 11n | dualband | 4102] | <ap_serial> [clients | static_config | config
| radio1 | radio2 | version]]
```

Parameters

access	Displays the status of the Wireless APs
registration	Displays the registration information
version	Displays the software version installed on Wireless APs.
load-groups	Displays the configured load groups.
defaults	Displays the Dynamic Radio Frequency management settings
config	Displays the configured values of the Wireless AP
standard	Displays the configured values of standard AP (AP2610/AP2620)
11n	Displays the configured values of the 802.11n Wireless APs (AP3610/ AP3620)
dualband	Displays the configured values of dualband.
4102	Displays the configured values of the RBT-4102 access point.
<ap_serial>	Specifies the serial number of a specific Wireless AP
clients	Displays the clients connected to the Wireless AP
static_config	Displays the static configuration values
config	Displays the configured values for the Wireless AP
radio1	Displays the Wireless AP's radio 1 settings
radio2	Displays the Wireless AP's radio 2 settings
version	Displays the software version and hardware type of the Wireless AP

Examples

The following example displays the serial number, name, and platform of connected Wireless APs.

```
EWC.enterasys.com# show ap
serial 0500008043050356 0500008043050356 AP3610 AP3600
serial 0500005432050511 0500005432050511 AP2610 AP2600
serial 0500006092051397 0500006092051397 AP2620 AP2600
serial 0500005432050445 0500005432050445 AP2610 AP2600
serial 0500006372051094 0500006372051094 AP2620 AP2600
serial 0002000003432212 Scalance VeriWave 2212 W786-2PROe W786
serial 0500005432050540 0500005432050540 AP2610 AP2600
serial 0500008083050056 AP3620 External VeriWave 0056 AP3620 AP3600
serial 0500006372051039 AP2620 External VeriWave 1039 AP2620 AP2600
serial 0500006372051125  AP2620 External VeriWave 1125 AP2620 AP2600
```

The following example displays the registration status of the Wireless APs

```
EWC.enterasys.com# show ap access
0122003880188015  LOCAL  APPROVED
0409920201204003 LOCAL  APPROVED
```

The following example displays the registration information

```
EWC.enterasys.com# show ap registration
security off
dinterval 1
dretry 3
```

The following example displays the clients connected to the Wireless AP with the serial 0409920201204003

```
EWC.enterasys.com# show ap 0409920201204003 clients
```

Client IP	Client MAC	User	Time Conn.	BSS MAC	SSID	Authentication	Privacy	Filter	Protocol	Pkts Sent	Pkts Recvd	Bytes Sent	Bytes Recvd
172.16.50.250	00:40:96:AB:61:58	-	00:04:00	00:0F:BB:09:F6:A2	CNL-103-CPx	Ext CP	WPA-PSK	Global	a	6	48	883	4937
Total										6	48	883	4937

The following example displays the static configuration values of the Wireless AP

```
EWC.enterasys.com# show ap 0409920201204003 static_config
Static IP Address: 10.205.0.11
Static Netmask:    255.255.255.0
Static Gateway:    10.205.0.2
AC IP: 10.205.0.1
AC Order: 1
```

The following example displays the configuration information of the Wireless AP with the serial number 0122003880188015.

```
EWC.enterasys.com# show ap 0500006072051201 config
AP Serial Number: 0500006072051201
AP host name: AP2620-0500006072051201
AP Name: 0500006072051201
Description:
Active # of clients: 0
AP software version: 07.41.03.0003
Port IP: 10.215.0.11
Status: approved
role : ap
Home: local
DHCP IP address: 10.115.3.15
DHCP NetMask: 255.255.255.0
DHCP Gateway: 10.115.3.2
Hardware Type:  Wireless AP2620-1 External-1
Wired MAC address: 00:0F:BB:09:06:F1
```

The following example displays the Wireless AP's radio 1 settings

```
EWC.enterasys.com# show ap 0500006072051201 radio1
dtim  5
beaconp 100
nonUnicastQuota 100
rts 2346
frag 2346
domain  MyDomain
channel 0(-1)
current channel 0(0)
last requested channel 0(0)
tx_max_power 18 dBm
divtx alternate
divrx best
hwretries  00000
radio mode off
no atpc
minbrate 6
maxbrate 24
maxoprate 54
max-distance 100
current_power: 0
dcs mode off
channel_plan all
```

The following example displays the Wireless AP's radio 2 setting

```
EWC.enterasys.com# show ap 0122003880188015 radio2
```

```
dtim  5
beaconp 100
nonUnicastQuota 100
rts 2346
frag 2346
domain  MyDomain
channel
current channel 0(0)
last requested channel 0(0)
divtx alternate
divrx best
preamble long
tx_max_power 18 dBm
hwretries  00000
radio mode b
no atpc
minbrate 1
maxbrate 11
maxoprate 54
max-distance 100
current_power: 18
dcs mode off
channel_plan auto
```

The following example displays the software version and hardware type for the Wireless AP.

```
EWC.enterasys.com# show ap 0500006072051201 version
Software version: 07.41.01.0003
Hardware Type: Wireless AP2620-1 External-1
```

The following example displays the software version installed on all Wireless APs.

```
EWC.enterasys.com# show ap version
Serial: 1000008239080585                Version: 07.41.01.0186
Serial: 0500008043050236                Version: 07.41.01.0186
Serial: 0500005230000824                Version: 07.41.01.0186
Serial: 100000549D080029                Version: 07.41.01.0186
Serial: 0500008043050251                Version: 07.41.01.0186
```

The following example displays the load groups.

```
EWC.enterasys.com# show load-groups
Load Groups:
Name: CNL_201_Radio-001                 Type : radio
Name: CNL_201_Client_Balancing-002      Type : client
Name: CNL_201_Radio-008                 Type : radio
Name: Radio-001                         Type : radio
Name: CNL_201_Client_Balancing-001      Type : client
```

3.21.4 show ap_certificate

Use the **show ap_certificate** command to displays the Wireless AP's current certificate credentials.

Syntax

```
show ap_certificate <ap_serial>
```

Parameters

ap_serial	Specifies Wireless AP's serial number

Examples

```
EWC.enterasys.com# show ap_certificate 0409920201204043
User: 0409920201204043
Password: ********
ap_serial: 0409920201204043
Certificate serial number: 51F5F66D000000000238
Issued on: Sat May 26 10:45:19 2007
Expire on: Sat Feb 21 18:25:02 2009
Issued by: CN=Seasametechtrial, DC=com, DC=extremenetworks, DC=techtrial
Full distinguished name: CN=0409920201203801
Subject alternative name:
```

3.21.5 show ap_certreq

Use the **show ap_certreq** command to display the available certificate signing request for the 802.1x EAP-TLS (Proxy mode) configuration.

Syntax

```
show ap_certreq
```

Parameters

None

Examples

```
EWC.enterasys.com# show ap_certreq
1: 0409920201203894.CSR
```

3.21.6 show ap_inventory

A report of Wireless APs connected to the Enterasys Wireless Controller can be displayed. This includes information about the Wireless AP's hardware, software, and connection status.

Use the **show ap_inventory** command to display a report of the Wireless APs with a pending or approved status on the Enterasys Wireless Controller.

Syntax

```
show ap_inventory
```

Parameters

None

Examples

The following example displays the Wireless APs connected to the Enterasys Wireless Controller.

```
EWC.enterasys.com# show ap_inventory
Name:            0002000007515340
Serial:          0002000007515340
Desc:
Status:          approved
Software:        V5 R3.10007.0
Hardware:        A&D Scalance W786-2HPW-Internal
Wired MAC:       00:0E:8C:8F:E5:B1
Poll Timeout:    15
Poll Interval:   3
Persistent:       off
Broadcast Dissoc:  off
Client Session Maintain:enabled
Assn:            Others
Static IP:       10.208.0.249
Netmask:         255.255.255.0
Gateway:         10.208.0.2
AC Search List:  -

Radio Settings          Radio b/g    Radio a

802.11a                 -            on
802.11b                 on           -
802.11g                 on           -
DTIM Period             5            5
Beacon Period           100          100
RTS/CTS Threshold       2346         2346
Frag. Threshold         2346         2346
Channel                 0            0
Power Level             18           18
Min Basic Rate          1            6
Max Basic Rate          11           24
Max Operational Rate    54           54
ATPC                    disabled     disabled
TX Power Adjust         0            0
TX Min Power            8            0
TX Max Power            18           18
Max Operational Rate    54           54
TX Diversity            Best         Best
```

```
RX Diversity            Best         Best
Preamble                Long         -
No of Retries BK        0            0
No of Retries BE        0            0
No of Retries VI        0            0
No of Retries VO        0            0
No of Retries TVO       0            0
Protection Mode         Auto         -
Protection Rate         11 Mbps      -
Protection Type         CTS only     -

BSS:MAC (radio bg)
--
BSS:MAC (radio a)
--
```

3.21.7 show apup

Use the **show apup** command to display all available upgrade images for Wireless APs on the Enterasys Wireless Controller by order of platform type.

Syntax

```
show apup [<platform>]
```

Parameters

<platform>	Specifies the platform of the Wireless AP

Examples

The following example displays the upgrade images currently available for the Wireless APs

```
EWC.enterasys.com# show apup
AP2600
1: AP200-07.41.01.0186.img
AP2600-1
1: AP200-07.41.01.0186.img
AP2605
1: AP200-07.41.01.0186.img
AP2650
1: AP2650-07.41.01.0186.img
AP2650-1
1: AP2650-07.41.01.0186.img
AP2650-2
1: AP2650-07.41.01.0186.img
AP3600
1: AP3600-07.41.01.0186.img
```

```
AP3600-1
1: AP3600-07.41.01.0186.img
AP3605
1: AP3600-07.41.01.0186.img
AP3630-NAM
1: AP3600-07.41.01.0186.img
AP3660
1: AP3600-07.41.01.0186.img
AP4102
1: AP4102-07.41.01.0186.img
AP4102C
1: AP4102-07.41.01.0186.img
W786
1: W786-07.41.01.0186.img
W786-1
1: W786-07.41.01.0186.img
W786-2
1: W786-07.41.01.0186.img
W788
1: W788-07.41.01.0186.img
```

The following example displays the upgrade images available for the W788 platform only

```
EWC.enterasys.com# show apup W788
W788
1: W788-07.41.01.0186.img
```

3.21.8 show audits

Use the **show audits** command to display audit information for the Enterasys Wireless Controller.

Syntax

```
show audits [next]
```

Parameters

next	Displays next screen containing audit information

Examples

The following example displays audit information for the Enterasys Wireless Controller

```
EWC.enterasys.com# show audits
Msg 1: 04/06/06 12:12:51, admin, Sys Mgmt,  Maintain., Syslog settings have been
updated
Msg 2: 04/06/06 12:11:55, admin, Sys Mgmt,  Maintain., System log level changed
from [3] to [1]
Msg 3: 04/06/06 11:23:18, admin, CLI_vns,  general, Set vns group: create vns:
vns2;
```

3.21.9 show availability

Use the **show availability** command to display availability settings for the Enterasys Wireless Controller.

Syntax

```
show availability
```

Parameters

None

Examples

The following example displays availability settings for the Enterasys Wireless Controller

```
EWC.enterasys.com# show availability
pair paired
pairrole secondary
pairip 192.168.4.207
fast_failover enabled
link_timeout 2
sync-mu disabled
```

3.21.10 show backup

Use the **show backup** command to display a list of backup files available on the Enterasys Wireless Controller.

Syntax

```
show backup [<n>]
```

Parameters

<n>	Specifies the index number of a backup file on the list

Examples

The following example displays a list of all backup files on the Enterasys Wireless Controller.

```
EWC.enterasys.com# show backup
1: test-lab6.04102005.174541.zip
2: test-lab6.04102005.174554.zip
3: test-lab6.04102005.174608.zip
4: test-lab6.04102005.174619.zip
5: test-lab6.04102005.174627.zip
6: test-lab6.04102005.174814.zip
7: test-lab6.23112005.161059.zip
8: test-lab6.23112005.162103.zip
```

The following example displays the comment string associated with the fourth listed backup file

```
EWC.enterasys.com# show backup 4
```

```
Comment="Time for another backup"
Backup type="all"
Backup/Export saved from software version="C20-07.41.01.0186"
```

3.21.11 show bootrom

Use the **show bootrom** command to display the bootrom images available on the Enterasys Wireless Controller, by order of Wireless AP. Use the optional parameter to display bootrom images by individual platform.

Syntax

```
show bootrom [<platform>]
```

Parameters

<platform>	Specifies the platform of the image

Examples

The following example displays the bootrom images for all platforms supported by the Enterasys Wireless Controller

```
EWC.enterasys.com# show bootrom
AP2600
1: bootrom2_2_0.sys
W788
No bootrom image upgrade files available on system.
```

The following example displays the bootrom image for the AP2600 platform only

```
EWC.enterasys.com# show bootrom AP2600
1: bootrom2_2_0.sys
```

3.21.12 show cdrs

Use the **show cdrs** command to display a directory listing of the user's call detail records. Use the parameters to display the contents of the records.

Syntax

```
show cdrs [<dir>] [<filename>| <1-9600>]
```

Parameters

<dir>	Specifies the name of the directory you want to view
<filename>	Specifies the name of the file you want to view
<1-9600>	Specifies an item number from the file name list

Examples

The following example lists the folders containing the call detail records.

```
EWC.enterasys.com# show cdrs
```

```
20050921wed
20050922thu
20050923fri
20050929thu
20050930fri
20051103thu
```

The following example lists the file names within folder 20050921wed

```
EWC.enterasys.com# show cdrs 20050921wed
1: 20050921194016.dat
2: 20050921204353.dat
3: 20050921212300.dat
4: 20050921212431.dat
5: 20050921213022.dat
6: 20050921213053.dat
```

The following example selects a record by file name and displays its contents

```
EWC.enterasys.com# show cdrs 20050921wed 20050921194016.dat
-------------------------------------------------
    Acct-Session-Id = 4331ed220001
    User-Name = david@lab.webdomain.com
    Filter-Id = Default
    Acct-Interim-Interval = 1800
    Session-Timeout = 0
    Class = 0x5a59 670 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    Acct-Status-Type = 2
    Acct-Delay-Time = 108287
    Acct-Authentic = 1
    Framed-IP-Address = 0.0.0.0
    Connect-Info = 802.11a
    NAS-Port-Type = Wireless-802.11
    Called-Station-ID = 00:50:C2:23:A0:59
    Caling-Station-ID = 00:0E:35:CA:EC:4E
    Siemens-AP-Serial = 0122003880188006
    Siemens-AP-Name = 0122003880188006
    Siemens-VNS-Name = zone_qua
    Siemens-SSID = lab7_zone
    Acct-Session-Time = 574
    Acct-Output-Packets = 54
    Acct-Input-Packets = 558
    Acct-Output-Octets = 9814
    Acct-Input-Octets = 64865
    Acct-Terminate-Cause = 6
    Authenticated_time = Sep 21 2005 19:30:42
```

```
    Disassociation_time = Dec 31 1969 19:00:00
```

Optionally, the same record could be viewed by specifying its number on the filename list instead of by its filename, as follows

```
EWC.enterasys.com# show cdrs 20050921wed 1
```

3.21.13 show checkpoint

Use the **show checkpoint** command to display the current Check Point configuration settings.

Syntax

```
show checkpoint
```

Parameters

None

Examples

The following example displays Check Point configuration settings

```
EWC.enterasys.com# show checkpoint
cplog
cpip 1.1.1.1
elaport 18187
elalogint 100
elaretry 2000
elaq 1000
sicname sicnamesample
sicpwd test
```

3.21.14 show clients apserial

Use the **show clients apserial** command to display all clients connected to a specified Wireless AP.

Note: Use **show ap** to list the serial numbers of existing Wireless APs. For more information, see "3.21.3, show ap" on page 3-24.

Syntax

```
show clients apserial <ap_serial>
```

Parameters

<ap_serial>	Specifies the serial number of an Wireless AP

Examples

The following example lists the clients connected to the Wireless AP with the serial number 0001000418800008

```
EWC.enterasys.com# show clients apserial 0001000418800008
```

```
Clien Client Use Time     BSS  SSID Authe Privac Filter Proto Pkts  Pkts  Bytes Bytes
t IP  MAC    r   Conn.    MAC       ntica y             col   Sent  Recvd Sent  Recvd
                                    tion
172.1 00:40: -   00:04:0  00:  CNL- Ext   WPA-   Global a     6     48    883   4937
6.50. 96:AB:     0        0F:  103- CP    PSK
250   61:58              BB:  CPx
                         09:
                         F6:
                         A2
Total
                                                          6     48    883   4937
```

3.21.15 show clients vns

Use the **show clients vns** command to display all clients connected to a specified VNS.

Note: Use **show vnsmode** to list the VNS names used on the Enterasys Wireless Controller. For more information, see "3.21.50, show vnsmode" on page 3-62.

Syntax

```
show clients vns <vns_name>
```

Parameters

<vns_name>	Specifies the name of a Virtual Network Service on the Enterasys Wireless Controller

Examples

The following example lists the clients connected to the VNS using the name CNL-205-CPn

```
EWC.enterasys.com# show clients vns CNL-205-CPn
```

```
Clien Client Use Time     BSS  SSID Authe Privac Filter Proto Pkts  Pkts  Bytes Bytes
t IP  MAC    r   Conn.    MAC       ntica y             col   Sent  Recvd Sent  Recvd
                                    tion
172.1 00:40: -   00:04:0  00:0 CNL- Ext   WPA-   Global a     6     48    883   4937
6.50. 96:AB:     0        F:BB 103- CP    PSK
250   61:58              :09: CPx
                         F6:A
                         2
Total
                                                          6     48    883   4937
```

3.21.16 show run-config

Use the **show run-config** to display the system's current running configuration commands.

Syntax

```
show run-config
```

Parameters

None

3.21.17 show dns

Use the **show dns** command to display the DNS configuration.

Syntax

```
show dns [1-3]
```

Parameters

[1-3]	Specifies the position of the DNS server in the DNS servers list.

Examples

```
EWC.enterasys.com# show dns 1
dns 1 192.1.1.3
```

3.21.18 show export

Use the **show export** command to display all the exported *text* files that contain the controller's configuration, cdrs, logs, audit and rogue data or all of them.

Syntax

```
show export
```

Parameters

None

Examples

The following example displays all the exported *text* files that contain controller's configuration, cdrs, logs, audit and rogue data or all of them.

```
EWC.enterasys.com# show export
1: Test_lab213_V5R3.10007-avail.zip
2: export_lab213_V4R1.7.10_NAMO_ENT.zip
3: lab-213-g.11042008.140940.zip
4: lab-213-g.webdomain.com.07032008.144403.zip
```

Note: During the export process, the *text files*, containing the controller's configuration, cdrs, logs, audit and rogue data are zipped for which the files display *.zip* extension.
The configuration text files are displayed with *.cli* extension.

3.21.19 show flash

Use the **show flash** command to display whether the flash card is mounted or not.

Note: The **show flash** command is applicable only to the Enterasys Wireless Controllers that support flash devices.

Syntax

```
show flash <status|sysinfo|list>
```

Parameters

status	Displays whether the flash card is mounted or not
sysinfo	Displays the memory usage information of the flash card
list	Displays all the files on the flash card

Examples

The following example displays that the flash card is mounted.

```
EWC.enterasys.com# show flash status
flash mounted
```

The following example displays the following memory usage information of the flash card:

- Size – Total capacity of the flash card.
- Used – Space used so far.
- Available – Space available for use.
- Use % – Space used in percentage.

```
EWC.enterasys.com# show flash sysinfo
Size    Used    Available    Use %
3.9G    32k     3.9G         1%
```

The following example displays the list of files that are saved on the flash card.

```
EWC.enterasys.com# show flash list
AC-MV-gxs-V5R3.10007.0-1.tar
gxs-V5R3.10007.0-1-rescue.tgz
```

3.21.20 show healthpoll

Use the **show healthpoll** command to display the current Health Poll Checking setting.

Syntax

```
show healthpoll
```

Parameters

None

Examples

The following example displays the current Health Poll Checking setting.

```
EWC.enterasys.com# show healthpoll
healthpoll enable
```

3.21.21 show import

Use the **show import** command to display all the imported *text* files that contained the controller's configuration, rogue data or both.

Syntax

```
show import
```

Parameters

None

Examples

The following example displays all the imported *text* files that contain the controller's configuration, cdrs, logs, audit and rogue data.

```
EWC.enterasys.com# show import
1: Test_lab213_V5R3.10007-avail.zip
2: export_lab213_V4R1.7.10_NAMO_ENT.zip
3: lab-213-g.11042008.140940.zip
4: lab-213-g.11042008.141154.zip
5: lab-213-g.11042008.141200.zip
6: lab-213-g.webdomain.com.07032008.144403.zip
```

3.21.22 show import_status

Use the **show import_status** command to display the import status of the text file, containing the controller's configuration, CDRs, logs, audit information and rogue data.

Syntax

```
show import_status
```

Parameters

None

Examples

The following example displays the import status of the text file, containing the controller's configuration, CDRs, logs, audit information and rogue data.

```
EWC.enterasys.com# show import_status
Import is in progress ……
Current status is 60%
```

The following example displays the import status when the import of the text file is not running.

```
EWC.enterasys.com# show import_status
```

```
Import process is not started
```

3.21.23 show key

Use the **show key** command to display the current product registration key information.

Syntax

```
show key
```

Parameters

None

Examples

The following example displays the current product registration key settings

```
EWC.enterasys.com# show key
Current Product Key Settings:
Locking ID: 00-1A-E8-10-06-19
Regulatory Domain: North America
Product Name: C20 Office
Number of Licensed APs: 16
Dynamic Radio Management: Enabled
External Captive Portal: Enabled
Activation key string : PRDKNAM-SBPXKCGH-N8FKS8A7-VYPK7CB3-OJD7RFP6
External Captive Portal Option Key:  EXTCP-308RRCDN-HFCVNZJV-HDGUK8BI-VCA6L1B6
Capacity Enhancement Option Keys:
- CAPC20-XJFH3126-IF977Z87-UD2RKDZR-7DBLQ10K
```

3.21.24 show l2ports

Use the show l2ports command to display the properties of the Layer 2 ports.

Syntax

```
show l2ports
```

Parameters

None

Examples

The following example displays the Layer 2 ports of a C2400 Controller.

```
EWC.enterasys.com# show l2ports

Status  Enable   Port   MAC               VLAN Physical  VLAN Service

UP      enable   esa0   08:00:06:81:C2:7D  U
DOWN    enable   esa1   08:00:06:81:C2:7E  U
DOWN    enable   esa2   08:00:06:81:C2:7F  U
```

```
DOWN    disable  esa3   08:00:06:81:C2:80  U
UP      enable   admin  08:00:06:85:91:AD
```

3.21.25 show lanset

Use the **show lanset** command to display the ports' speed — the data transmission rate of an output/input channel on each port

Syntax

```
show lanset
```

Parameters

None

Examples

The following example displays the lanset settings of a C2400 Controller.

```
EWC.enterasys.com# show lanset
Port name:              admin
Port Auto Negotation:   On
Port Speed:             Any
Port Duplex:            Both

Port Name:              lan1
Port Auto Negotation:   On
Port Speed:             Any
Port Duplex:            Both

Port Name:              lan2
Port Auto Negotation:   On
Port Speed:             Any
Port Duplex:            Both

Port Name:              lan3
Port Auto Negotation:   On
Port Speed:             Any
Port Duplex:            Both

Port Name:              lan4
Port Auto Negotation:   On
Port Speed:             Any
Port Duplex:            Both
```

3.21.26 show log

Use the **show log** command to display logs and reports for the Enterasys Wireless Controller.

Syntax

```
show log <log_name> | [[first | last] <number>]
```

Parameters

log_name	The log that you want to view: • ospf-neighbor • ospf-linkstate • dhcp • upgradeLog.txt • auditRecords.log • upgrade.log • configChanges.log
first	Indicates that the first records in the log will be displayed
last	Indicates that the last records in the log will be displayed
<number>	Specifies the number of logs to display from the file

Examples

The following example displays the first two records from the auditRecords log file

```
EWC.enterasys.com# show log auditRecords.log first 2
 5516324453019803260admin                  CLI_controller           general
keyconfigurationchanged:activateTRDKNAM-NCF47ABS-I1BVRP9U-SGDKVBFR-NFBQ6ZJQ,
 5516324457314024504admin                CLI_system_management      general
downloading import file from server 192.168.3.108
```

The following example displays the last five DHCP log messages

```
EWC.enterasys.com# show log dhcp last 5

Timestamp          DHCP Message

Sep 13 20:33:14    dhcpd: DHCPACK to 172.21.177.21 (00:11:95:ec:a7:c0) via esa9
Sep 13 20:34:53    dhcpd: DHCPINFORM from 172.21.177.21 via esa9
Sep 13 20:34:53    dhcpd: DHCPACK to 172.21.177.21 (00:11:95:ec:a7:c0) via esa9
Sep 13 20:34:56    dhcpd: DHCPINFORM from 172.21.177.21 via esa9
Sep 13 20:34:56    dhcpd: DHCPACK to 172.21.177.21 (00:11:95:ec:a7:c0) via esa9
```

The following example displays log entries from OSPF neighbors

```
EWC.enterasys.com# show log ospf-neighbor

Neighbor RouterID    Router Priority    State      IP           Interface

192.168.12.7         1                  Full/DR    10.91.0.2    esa0:10.91.0.1
```

The following example displays the log entries for the OSPF linkstate database

```
EWC.enterasys.com# show log ospf-linkstate

Router LSA (Type 1):

Link ID          Advertising Router    Age     Sequence No    Checksum    Link Count

192.168.4.202    192.168.4.202         1460    0x80000085     0x8f18      3
```

The following example displays the log entries for upgradeLog.txt.

```
EWC.enterasys.com# show log upgradeLog.txt
OS-7_31_0-7

Wed Mar 19 14:21:48 EDT 2008 OS-5_1_8-1
Installing rpm of version V5R1.10034.0 on Wed Mar 19 14:21:53 EDT 2008
Tue Mar 10 12:39:04 EDT 2009 OS-5_3_17-1
Installing rpm of version V5R3.10034.0 on Tue Mar 10 12:39:11 EDT 2009
Mon Jun 1 10:52:53 EDT 2009 OS-6_0_19-1
Installing rpm of version V6R0.10019.0 on Mon Jun  1 10:52:59 EDT 2009
Thu Aug 20 14:47:27 EDT 2009 OS-6_1_8-1
Installing rpm of version V6R1.10029.0 on Thu Aug 20 14:47:39 EDT 2009
Installing rpm of version V6R1.10602.0 on Mon Sep 13 05:11:30 EDT 2010
Installing rpm of version 07.41.01.0122T on Mon Sep 13 05:31:02 EDT 2010
EWC.enterasys.com#
```

The following example displays the log entries for upgrade.log.

```
EWC.enterasys.com# show log upgrade.log
Sep 13 05:30:47 EDT 2010 From: V6R1.10602.0 To: 07.41.01.0122T
Sep 13 05:30:47 EDT 2010 C20 Upgrading From Release 6_1
Sep 13 05:35:05 EDT 2010 Successfully imported license
Sep 13 05:35:21 EDT 2010 Successfully EWC.enterasys.com:d the Configuration
Sep 13 05:35:22 EDT 2010 Successfully Performed Rogues EWC.enterasys.com:
Sep 13 05:35:22 EDT 2010 Successfully Performed Netsight Import
EWC.enterasys.com#
```

The following example displays the log entries for configChanges.log.

```
EWC.enterasys.com# show log configChanges.log
CLI Import/EWC.enterasys.com: start: Tue Sep 14 00:27:57 2010


CLI Import/EWC.enterasys.com: end: Tue Sep 14 00:28:16 2010
EWC.enterasys.com#
```

3.21.27 show loglevel

Use the **show loglevel** command to display the system log level of the Enterasys Wireless Controller or the Wireless AP.

Syntax

```
show loglevel (ac|ap)
```

Parameters

ac	Displays the log level of the Enterasys Wireless Controller
ap	Displays the log level of the Wireless AP

Examples

The following displays the system log level of both the Enterasys Wireless Controller and the Wireless AP

```
EWC.enterasys.com# show loglevel
Ac Log level: Informational (4)
Ap Log level: Critical (1)
```

The following displays the system log level of the Enterasys Wireless Controller only

```
EWC.enterasys.com# show loglevel ac
Ac Log level: Informational (4)
```

The following displays the system log level of the Wireless AP only

```
EWC.enterasys.com# show loglevel ap
Ap Log level: Critical (1)
```

3.21.28 show ospf

Use the **show ospf** command to display the system's Open Shortest Path First (OSPF) interfaces and configuration.

Syntax

```
show ospf (interface|neighbors|config|database)
```

Parameters

interface	Displays the details of all current OSPF interfaces
neighbors	Displays the OSPF neighbors the Enterasys Wireless Controller has adjacency with

config	Displays the OSPF configuration details
database	Displays the OSPF linkstate database

Examples

The following example displays the details of all OSPF interfaces

```
EWC.enterasys.com# show ospf interface
OSPF Interface #0:
    Port Name            :esa0
    OSPF Status          :Enabled
    OSPF authentication  :None
    Link Cost            :10
    Hello Interval       :10
    Dead Interval        :40
    Retransmit Interval  :5
    Transmit Delay       :1
```

The following example displays the details of all OSPF neighbors

```
EWC.enterasys.com# show ospf neighbors
Neighbor ID    Router ID      Priority    State      IP Address    Interface
1             192.168.4.3    1          Full/DR    10.209.0.2    esa0:10.209.0.1
```

The following example displays all OSPF configuration data

```
EWC.enterasys.com# show ospf config
OSPF Area            :0.0.0.5
OSPF Area Type       :default
OSPF Router ID       :
OSPF Protocol Status :enable
```

The following example displays OSPF information from a database

```
EWC.enterasys.com# show ospf database
Router LSA (Type 1):
Link ID        Advertising Router    Age     Sequence No    Checksum    Link Count
10.203.1.2      10.203.1.2           1745    0x800001c3     0xae1f      17
10.206.0.1      10.206.0.1           1525    0x8000009d     0x782e      3

Network LSA (Type 2):
Link ID       Advertising Router    Age     Sequence No    Checksum
10.109.0.2    192.168.4.3           334     0x800000a8     0x781d
10.203.0.2    192.168.4.3           334     0x80000713     0xb73a

Network Summary LSA (Type 3):
Link ID         Advertising Router    Age     Sequence No    Checksum    Route
10.2.0.0      192.168.4.3         76     0x80000080    0xd36a     10.2.0.0/24
10.2.0.0      192.168.4.9         969    0x8000007f    0xb187     10.2.0.0/24
```

```
ASBR Summary LSA (Type 4):
Link ID         Advertising Router     Age      Sequence No    Checksum
10.203.1.2      192.168.4.3            1324     0x8000002b     0xd1f4
10.203.1.2      192.168.4.9            970      0x8000002b     0xa31e

AS-External LSA (Type 5):
Link ID           Advertising Router    Age     Sequence No    Checksum    Route
0.0.0.0         192.1.5.115         806    0x80000030    0x160a     0.0.0.0/0
10.22.1.0       192.168.3.2         585    0x800006f1    0x30e9     10.22.1.0/24
```

3.21.29 show policy

Use the **show policy** command to display configuration information for all Polices configured on the Enterasys Wireless Controller.

Syntax

```
show policy
```

Examples

The following example displays configuration information about all configured Policies.

```
EWC.enterasys.com# show policy

Policy name        Topology        Ingress rate    Egress rate     Mode           Filter defined
                                   profile         profile

open               Seg1_Routed     no-change       no-change       routed         Yes
UnAuth             Seg2_Routed     no-change       no-change       routed         Yes
Auth               Seg2_Routed     no-change       no-change       routed         Yes
BAC                Bridged at AP   no-change       no-change       b@ap           Yes
                   untagged
```

3.21.30 show wlans

Use the **show wlans** command to display a list of all WLAN Services configured on the Enterasys Wireless Controller.

Syntax

```
show wlans
```

Examples

The following example displays information about all configured WLAN Services.

```
EWC.enterasys.com# show wlans

Name              Service Type   Enabled       SSID           Privacy       Auth Mode
```

```
Lab12-open        std           enabled       Lab12-open     none          disabled
Lab12-INT_CP      std           enabled       Lab12-INT_CP   none          internal
Lab12-1           std           enabled       Lab12-1        none          disabled
top-routed        std           enabled       aaaa           none          disabled
Lab12-EXT_CP      std           enabled       Lab12-EXT_CP   none          external
```

3.21.31 show report

Use the **show report** command to display a list of all activity reports on the Enterasys Wireless Controller, or detailed information within an individual report.

Syntax

```
show report [<report_name>]
```

Parameters

<report_name>	Specifies the report name from the list of activity reports

Examples

The following example displays a list of activity reports available on the Enterasys Wireless Controller.

```
EWC.enterasys.com# show report
reports:
active_clients
active_clients_by_vns
active_clients_by_wireless_apserial
active_wireless_aps
active_wireless_load_groups
admission_control_wireless_aps
ap_availability
clients_by_Current_HWC
clients_by_home
external_connection
mesh_wds_wlan_wireless_ap_stats
mobility_tunnel_matrix
policy_filter_stats
radius_stats
remotable_vns_information
remote_states
topology_filter_stats
topology_stats
wired_ap_stats
wireless_ap_stats
wireless_controller_port_statistics
```

The following example displays information contained within the external_connection report.

```
EWC.enterasys.com# show report external_connection
Connection Security Level
192.168.1.10 Open
192.168.3.25 Private
```

The following example displays information contained within the active_wireless_aps report

```
EWC.enterasys.com# show report active_wireless_aps
name: 0409920201201319
serial: 0409920201201319
AP IP: 10.7.0.54
Num Clients: 0
Home: LOCAL
Packets sent: 0
Packet Received: 0
Bytes Sent: 0
Bytes Received: 0
802.11b/g  Channel: 1  Power: 0
802.11a  Channel: 1  Power: 0
```

The following example displays clients connected to the home Enterasys Wireless Controller.

```
EWC.enterasys.com# show report clients_by_home
ac_ip 10.109.0.1
ac_ixp_addr 10.109.0.1
ac_desc C20-37
mu_ip 172.22.214.30
mu_mac 00:03:7F:BF:16:9F
mu_user
home ip 10.109.0.1
Tunnel with 10.109.0.4 Disconnected
Tunnel with 10.209.0.1 Disconnected

ac_ip 10.109.0.4
ac_ixp_addr 10.109.0.4
ac_desc EWC
Tunnel with 10.209.0.1 Disconnected
Tunnel with 10.109.0.1 Disconnected

ac_ip 10.209.0.1
ac_ixp_addr 10.209.0.1
ac_desc EWC
Tunnel with 10.109.0.4 Disconnected
Tunnel with 10.109.0.1 Disconnected
```

The following example displays client connected to foreign Enterasys Wireless Controller.

```
EWC.enterasys.com# show report clients_by_foreign_EWC
```

```
ac_ip 10.109.0.1
ac_ixp_addr 10.109.0.1
ac_desc C20-37
mu_ip 172.22.215.27
mu_mac 00:14:6C:F6:A4:4E
mu_user wzhu
home ip 10.109.0.1
Tunnel with 10.209.2.1 Connected
Tunnel with 10.109.1.4 Connected
Tunnel with 10.109.0.5 Connected
Tunnel with 10.209.0.3 Connected

ac_ip 10.109.1.4
ac_ixp_addr 10.109.1.4
ac_desc EWC
Tunnel with 10.209.2.1 Connected
Tunnel with 10.109.0.1 Connected
Tunnel with 10.109.0.5 Connected
Tunnel with 10.209.0.3 Connected

ac_ip 10.209.0.3
ac_ixp_addr 10.209.0.3
ac_desc EWC
Tunnel with 10.109.0.1 Connected
Tunnel with 10.109.0.5 Connected
Tunnel with 10.109.1.4 Connected
Tunnel with 10.209.2.1 Connected

ac_ip 10.209.2.1
ac_ixp_addr 10.209.2.1
ac_desc EWC
Tunnel with 10.109.1.4 Connected
Tunnel with 10.109.0.1 Connected
Tunnel with 10.109.0.5 Connected
Tunnel with 10.209.0.3 Connected

ac_ip 10.109.0.5
ac_ixp_addr 10.109.0.5
ac_desc EWC207
Tunnel with 10.209.2.1 Connected
Tunnel with 10.109.1.4 Connected
Tunnel with 10.109.0.1 Connected
Tunnel with 10.209.0.3 Connected
EWC.enterasys.com#
```

3.21.32 show restore

Use the **show restore** command to display the archives that can be restored on the Enterasys Wireless Controller.

Syntax

```
show restore
```

Parameters

None

Examples

The following lists the restorable archives on the Enterasys Wireless Controller

```
EWC.enterasys.com# show restore
1: EWC.10112005.150257.zip
```

3.21.33 show routes

Use the **show routes** command to display the routing table or static routes of the Enterasys Wireless Controller.

Syntax

```
show routes (all|static)
```

Parameters

all	Displays the routing table
static	Displays the static routes

Examples

The following example displays the routing table

```
EWC.enterasys.com# show routes all
Dest Addr         Netmask           Gateway       Interface    RouteType    Status

0.0.0.0           0.0.0.0           10.7.0.2      esa0         Static       Active
10.7.0.0          255.255.255.0      None         esa0         Connected    Active
10.7.1.0          255.255.255.0      None         esa1         Connected    Active
127.0.0.0         255.0.0.0          None         lo           Kernel     Inactive
127.0.0.0         255.0.0.0         None          lo           Connected    Active
136.157.233.128    255.255.255.128    192.168.1.1   eth0         Kernel       Active
172.16.113.0      255.255.255.0      None         esa2         Connected    Active
172.16.114.0      255.255.255.0      None         esa3         Connected    Active
172.16.117.0      255.255.255.128    None         esa5         Connected    Active
172.16.117.128    255.255.255.128    None         esa6         Connected    Active
172.16.118.0      255.255.255.192    None         esa7         Connected    Active
172.16.118.64     255.255.255.192    None         esa8         Connected    Active
```

```
172.16.118.128    255.255.255.192    None          esa9        Connected    Active
172.16.118.192    255.255.255.192    None          esa4        Connected    Active
172.16.125.0      255.255.255.0      None          esa10       Connected    Active
```

The following example displays the static routes on the Enterasys Wireless Controller

```
EWC.enterasys.com# show routes static
RouteID    Dest Addr     Netmask     Next Hop     Interface     OverrideDynamic

1          0.0.0.0       0.0.0.0     10.7.0.2     1             on
```

3.21.34 show schedule_ backup

Use the **show schedule_backup** command to display the current scheduled backup settings.

Syntax

```
show schedule_backup
```

Parameters

None

Examples

```
EWC.enterasys.com# show schedule_backup
protocol ftp
server 192.168.4.81
user admin
password ******
dir /home/user/destdir
type all
freq daily everyday
starttime 02:00
```

3.21.35 show schedule_upgrade

Use **show schedule_upgrade** command to display the current scheduled upgrade settings.

Syntax

```
show schedule_upgrade
```

Parameters

None

Examples

```
EWC.enterasys.com# show schedule_upgrade
schld_upgrd 10:01:01:02 local AC-MV-07.41.03.0003-1.gps
upgrade_backup remote 192.168.4.121 test abc123 /tmp/v53 L103-C20-07.41.03.0003-
rescue-user.tgz
```

3.21.36 show snmp

Use the **show snmp** command to display the SNMP settings for the Enterasys Wireless Controller.

Syntax

```
show snmp
```

Parameters

None

Examples

The following example displays the SNMP settings for the Enterasys Wireless Controller.

```
EWC.enterasys.com# show snmp
SNMP v1/v2
contact Bill Smith
location lab-91
rcommunity public
rwcommunity private
context
severity 4 (informational)
port 162
publish-ap enable

trap-manager-v1v2 1 136.157.233.176
trap-manager-v1v2 2 192.168.3.108
no SNMPv3 trap1 destination
no SNMPv3 trap2 destination
```

3.21.37 show stats

Use **show stats** to display throughput related statistics for the Wireless APs and for the Enterasys Wireless Controller interfaces.

Note: Use **show ap** to list the serial numbers of existing Wireless APs. For more information, see "3.21.3, show ap" on page 3-24.

Syntax

```
show stats (ap (<ap_serial> [wired | wireless (radio1 | radio2)]) | interface
<interface_name>)
```

Parameters

ap	Displays properties of an Wireless AP
<ap_serial>	Specifies the serial number of an Wireless AP
wired	Displays the hardwired connection
wireless	Displays the wireless connection

radio1	Displays radio1 statistics
radio2	Displays radio2 statistics
interface	Displays properties of a port on the Enterasys Wireless Controller
<interface_name>	Specifies the name of a port on the Enterasys Wireless Controller

Examples

The following example displays statistics for the Wireless AP 0001000418800008

```
EWC.enterasys.com# show stats ap 0001000418800008
Serial:           0409920201203917
IP Address:       10.222.0.126
Clients:          1
Home:             local
Session start:    2008-06-18 19:30:50
Uptime:           9878.13333333 min
Packets Sent:     419350
Packets Received: 936371
Bytes Sent:       110108177
Bytes Received:   428278710
Protection Mode: on
802.11b/g Ch/Tx:  2462  /15
802.11a Ch/Tx:    5200 /16
```

The following example displays the statistics for the same Wireless AP over its wired connection

```
EWC.enterasys.com# show stats ap 0001000418800008 wired
IP Address:     10.222.0.126
Status:         approved

Statistics           Receive      Transmit

Discarded Packets    1661         0
Total Errors         0            0
Unicast Packets      645614       419231
Multicast Packets    201404       3
Broadcast Packets    90139        488
Total Packets        0            419722
Total Bytes          428661221    110236012
```

The following example displays the statistics for Wireless AP 0500006072051204 over the radio1 wireless connection.

```
EWC.enterasys.com# show stats ap 0500006072051204 wireless radio1

Mode: a

MAC Address: 00:0F:BB:09:EC:E0
```

```
MAC Address: 00:0F:BB:09:EC:E1
MAC Address: 00:0F:BB:09:EC:E2
MAC Address: 00:0F:BB:09:EC:E3
MAC Address: 00:0F:BB:09:EC:E4

SSID: CNL-91-0-0-ssid
SSID: CNL-91-0-1-ssid
SSID: CNL-91-0-2-ssid
SSID: CNL-91-0-3-ssid
SSID: CNL-91-WDS-ssid
Operational Max Rate: 54
Channel: 157:5785MHz
Current Power Level(dBm): 0
IP Address:     10.91.0.50
Status:         approved
There are no active clients on this radio
There are 1 WDS Children.


Statistics                Received   Transmitted

Discarded Packets         1          1
Errors                    82519      1
Unicast Packets           0          46605
Multicast Packets         0          0
Broadcast Packets         0          0
Total Successful Packets  0          46605
Total Successful Bytes    727933     6815737


Statistics                                          802.11 MIB Values

WEP ICV Error Count                                 0
WEP Excluded Count                                  0
Retry Count                                         0
Multiple Retry Count                                0
RTS Success Count                                   0
RTS Failure Count                                   0
ACK Failure Count                                   609
Frame Duplicate Count                               1
Transmitted Fragment Count                          5312
Multicast Transmitted Frame Count                   0
Failed Count                                        1
Received Fragment Count                             46605
Multicast Received Frame Count                      0
```

```
FCS Error Count                                          124944
WEP Undecryptable Count                                  0
Deauthentications Due to CAC                             0
DCS Channel Utilization by Adjacent AP`s [%] - Average   n/a
DCS Channel Utilization by Adjacent AP`s [%] - Maximum   n/a
DCS Tx Channel Utilization [%] - Average                 n/a
DCS Tx Channel Utilization [%] - Maximum                 n/a
DCS Rx Channel Utilization [%] - Average                 n/a
DCS Rx Channel Utilization [%] - Maximum                 n/a
DCS Noise [dBm] - Average                                n/a
DCS Noise [dBm] - Maximum                                n/a
```

The following example displays the statistics for the interface esa0.

```
EWC.enterasys.com# show stats interface esa0
Frames Transmitted:             466898
Frames Received:                673553
Octets Transmitted:             105750978
Octets Received:                131981692
Multicast Frames Transmitted:   11
Multicast Frames Received:      1419
Broadcast Frames Transmitted:   2852
Broadcast Frames Received:      1197
Pause Frames Transmitted:       0
Pause Frames Received:  0
Frame Check Sequence Error:     0
Frame Too Long Errors:          0
```

3.21.38 show syslog

Use the **show syslog** command to display system log levels.

Syntax

```
show syslog
```

Parameters

None

Examples

The following example displays the current system log levels

```
EWC.enterasys.com# show syslog
syslogip 1  192.168.3.106 enable
syslogip 2  192.168.4.129 enable
syslogip 3  192.168.4.200 enable
svcmsg
audmsg
facility application 0
```

```
facility service 4
facility audit 6
```

3.21.39 show system_state

Use the **show system_state** command to display the Enterasys Wireless Controller's system information.

Syntax

```
show system_state process | cpu | memory | disk | mgmt | uptime | info
|manufacturing
```

Parameters

process	Displays the current CPU and memory usage of system processes
cpu	Displays the amount of CPU usage
memory	Displays the amount of memory being used on the system
disk	Displays the hard-disk usage by folder
mgmt	Displays the system management settings
uptime	Displays the amount of time the system has been running continuously
info	Displays the information on various processes run by the system
manufacturing	Displays hardware information about the controller

Examples

The following example displays the current processes running on the system

```
EWC.enterasys.com# show system_state process
PID      Process Name             State       % CPU    % Mem

1123     VN Manager               S           0.0      0.9
8010     NSM Server               S           0.0      0.6
16527    Config Manager           S           0.0      1.6
1425     CLI                      S           0.0      3.5
-        OSPF Server              inactive    -        -
-        Remote INS               inactive    -        -
15891    Langley                  S           0.0      0.5
520      MySQL Server             S           0.0      9.7
1111     RU Manager               S           0.0      0.9
15893    SNMP Agent               S           0.0      0.5
-        RF Data Collector        inactive    -        -
23758    Radius Client            S           0.0      0.5
960      Stats Server             S           0.0      0.6
16566    Security Manager         S           0.0      0.9
656      Event Server             S           0.0      1.4
548      Startup Manager          S           0.0      0.5
```

```
1131     RU Session Manager       S          0.0      0.5
974      Host Services Manager    S          0.0      2.3
1117     Radius Accounting        S          0.0      0.4
-        DHCP                     inactive   -        -
990      Test Client              S          0.0      0.4
1129     LLC Handler              S          0.0      0.6
```

The following example displays the CPU usage on the system

```
EWC.enterasys.com# show system_state cpu
CPU states:  1.5% user,  1.5% system,  0.0% nice,  6.8% idle
```

The following example displays the memory usage on the system

```
EWC.enterasys.com# show system_state memory
Mem:   247372K av,  235516K used,   11856K free,       0K shrd,   67528K buff
Swap: 1028120K av,    6368K used, 1021752K free                   85756K cached
```

The following example displays the hard disk usage (C1000 platform)

```
EWC.enterasys.com# show system_state disk
Partition    Total Space    Used      Available    Use %

root         26873436       938116    24570200     4%
home         2016016        32860     1880744      2%
cdr          2016044        32816     1880816      2%
logs         1510032        169984    1263340      12%
reports      1510032        32816     1400508      3%
trace        1510032        32816     1400508      3%
```

The following example displays the hard disk usage (C2400 platform)

```
EWC.enterasys.com# show system_state disk
Partition    Total Space    Used      Available    Use %

root         608756         380624    197208       66%
images       208616         120249    77927        61%
log          119783         4845      108916       5%
cdr          31083          1032      28447        4%
tmp          131072         20504     110568       16%
```

The following example displays the system management settings

```
EWC.enterasys.com# show system_state mgmt
AC software version: 5.3
AC software build: V5 R3.10014.0
AC hardware platform version: Revision 2
Product Name: C1000
Hostname: lab-119-g
Domain: webdomain.com
IP Address: 192.168.4.32
Subnet Mask: 255.255.255.0
Mgmt Gateway: 192.168.4.11
```

```
Primany DNS: 1.1.1.1
Secondary DNS: 2.2.2.2
Time Zone: America/Montreal
Country: CA
```

The following example displays system uptime

```
EWC.enterasys.com# show system_state uptime
System uptime: 6 days, 1:49
```

3.21.40 show tech_support

Use the **show tech_support** to display a list of technical support files available on the system.

Note: Use **tech_support** to generate technical support files. For more information, see "3.23, tech_support" on page 3-64.

Syntax

```
show tech_support
```

Parameters

None

Examples

The following example displays the available technical support files

```
EWC.enterasys.com# show tech_support
1: tech-ac.tar.gz
2: tech-all.tar.gz
3: tech-ap.tar.gz
4: tech-log.tar.gz
```

3.21.41 show time

Use the **show time** command to display the system time.

Syntax

```
show time
```

Parameters

None

Examples

The following example displays the system time and time server settings

```
EWC.enterasys.com# show time
Fri Apr 17 11:49:24 EDT 2009
```

3.21.42 show time-config

Use the **show time-config** command to display the system time and time server settings.

Syntax

```
show time-config
```

Parameters

None

Examples

The following example displays the system time and time server settings

```
EWC.enterasys.com# show time-config
ntp: internal ntp server
ntpip 1 192.168.4.84
ntpip 2 192.168.4.89
ntpip 3 200.200.200.200
tz America/Montreal
```

3.21.43 show topology

Use the **show topology** command to display the IDs and names of IP interfaces.

Syntax

```
show topology [l3]
```

Parameters

l3	Displays only topologies with an L3 configuration. The topologies are listed by index number.

Usage

You can identify an IP using its interface name or, for short, the identifier returned by the **show topology l3** command. Interface name is the name of any topology with L3 configuration (Physical, Admin, B@AC or Routed).

Examples

The following example displays the output of the **show topology** command when run without additional parameters

```
EWC.enterasys.com# show topology

Name                    Mode        L2:VlanId,port    L3:IP,GW,DHCP

Admin                   admin       N/A,Admin         192.168.4.37,192.168.4.
                                                      11,N/A
```

```
esa0                        physical    545,esa0          10.109.0.1,10.0.0.2,non
                                                          e
esa1                        physical    -1,esa1           10.0.1.1,10.0.1.2,none
Bridged at AP untagged      b@ap        -1,N/A
Enterasys-37Topology        b@ac        647,esa0          10.209.2.37,0.0.0.0,non
                                                          e
777                         b@ac        777,esa-1
649                         b@ac        649,esa-1
650                         b@ac        650,esa0


Topology global info:
Internal VLAN ID: 1
Multicast support:
disabled
```

Examples

The following example uses the **show topology l3** command to obtain interface information for use with the ping or traceroute commands

```
EWC.enterasys.com# show topology l3

Name                                Mode              L3:IP

1:Admin                             admin             192.168.4.37
2:esa0                              physical          10.0.0.1
3:esa1                              physical          10.0.1.1
4:Enterasys-37Topology              b@ac              10.10.1.1
5:CNL-209-AAA:engineering           routed            172.22.2.1
```

3.21.44 show traffic_capture

Use the **show traffic_capture** command to display the status of traffic capture.

Syntax

```
show traffic_capture
```

Parameters

None

Examples

The following is the example of the status display when the traffic capture is running.

```
EWC.enterasys.com# show traffic_capture
capture is running
```

The following is the example of the status display when the traffic capture is stopped.

```
EWC.enterasys.com# show traffic_capture
capture is stopped
```

3.21.45 show upgrade

Use the **show upgrade** command to display all of the software upgrade images available on the Enterasys Wireless Controller.

Syntax

```
show upgrade
```

Parameters

None

Examples

The following example displays the upgrade images on the Enterasys Wireless Controller.

```
EWC.enterasys.com# show upgrade
1: AC-MV-07.41.03.0003-1.gps (flash)
```

Note: Files located on an external flash card have **(flash)** next to them. In the above example, the file `AC-MV-07.41.03.0003-1.gps (flash)` is located on the flash card.

3.21.46 show upgrade_backup_dest

Use the **show upgrade_backup_dest** command to display the settings of FTP server where the controller's existing image will be backed up.

Syntax

```
show upgrade_backup_dest
```

Parameters

None

Examples

```
EWC.enterasys.com# show upgrade_backup_dest
upgrade_backup_dest 192.168.4.181 admin abc123 / backupClone.tgz
```

3.21.47 show upgrade_history

Use the **show upgrade_history** command to display the software upgrade history.

Syntax

```
show upgrade_history
```

Parameters

None

Examples

```
EWC.enterasys.com#  show upgrade_history
Date    Type    Version
Thu Feb 24 11:41:00 EST 2011    Upgraded        07.41.01.0150
Tue Jan 11 10:36:44 EST 2011    Installed       07.41.01.0100T
Tue Jan 11 10:36:27 EST 2011    Installed       OS-7_41_0-7
```

3.21.48 show upgrade_image_src

Use **show upgrade_image_src** command to display the settings of FTP server where the controller's new image is located.

Syntax

```
show upgrade_image_src
```

Parameters

None

Examples

```
EWC.enterasys.com#  show upgrade_image_src
upgrade_image_src 192.168.4.10 admin abc123 /rpms AC-MV-07.41.03.0003-1.gxs
```

3.21.49 show users

Use the **show users** command to display the user and administrator accounts defined on the Enterasys Wireless Controller.

Syntax

```
show users
```

Parameters

None

Examples

The following example displays the users defined on the Enterasys Wireless Controller

```
EWC.enterasys.com# show users
ID     Privilege
admin  admin
test   admin
```

3.21.50 show vnsmode

Use the **show vnsmode** command to display all VNS information for every VNS on the Enterasys Wireless Controller.

Syntax

```
show vnsmode
```

Parameters

None

Examples

The following example displays a list of every VNS currently on the Enterasys Wireless Controller

```
EWC.enterasys.com# show vnsmode

VNS             Enabled   WLAN Service Authentica   Privacy  Default    Topology     Mode
                                       tion                  Policy

Lab12-open      enabled   Lab12-open   disabled     none     open       Seg1_Routed  routed
Lab12-INT_CP    enabled   Lab12-       internal     none     UnAuth     Seg2_Routed  routed
                          INT_CP
testvns         enabled   Lab12-1      disabled     none     Auth       Seg2_Routed  routed
3PAP            disabled  3PAP         disabled     none     3PAP       esa2         physi
                                                                                     cal
```

3.21.51 show vnsmode radius

Use the **show vnsmode radius** command to display configured RADIUS server information for the Enterasys Wireless Controller.

Syntax

```
show vnsmode radius
```

Parameters

None

Examples

The following example displays a list of every RADIUS server currently known by the Enterasys Wireless Controller.

```
EWC.enterasys.com# show vnsmode radius
Strict: disable
Radius MAC format:1.XXXXXXXXXXX

Name              IP address    Protocol   Retries      Timeout      Ports        Priority
                                           (Auth:Acct)  (Auth:Acct)  (Auth:Acct)  (Auth:Acct)

IAS               192.0.1.202   PAP        3:3          5:5          1812:1813    4:4
Lab               134.14.12.23  PAP        3:3          5:5          1812:1813    1:1
test-radius       10.10.10.10   PAP        3:3          5:5          1812:1813    5:5
```

3.21.52 show web

Use the **show web** command to display the web timeout time (in minutes) — the time after which the web session will time out.

Syntax

```
show web
```

Parameters

None

Examples

```
EWC.enterasys.com# show web
timeout 1:00
no showvns
guestportal-admin-timeout 0:01
```

Note: The web timeout time is displayed in *hh:mm* format. In the above example, the web timeout time is 1 hour.

3.22 shutdown

Use the **shutdown** command to stop or reboot the Enterasys Wireless Controller.

Syntax

```
shutdown (halt|reboot)
```

Parameters

halt	Stop the Enterasys Wireless Controller
reboot	Reboots the Enterasys Wireless Controller

Examples

The following example reboots the Enterasys Wireless Controller.

```
EWC.enterasys.com# shutdown reboot
```

3.23 tech_support

Use the **tech_support** command to create compressed technical support files containing system information. Use the **no** form of the command to delete them.

Note: Use **show tech_support** to display a list of technical support files created on the system. For more information, see "3.21.40, show tech_support" on page 3-58.

Syntax

```
tech_support [ap [nostats]|ac|log|all [nostats] [filename]]
```

```
no tech_support (<filename>|<number>)
```

Parameters

ap	Collects Wireless AP information
ac	Collects Enterasys Wireless Controller information
log	Collects log information
all	Collects Wireless AP, Enterasys Wireless Controller, and log information
<filename>	Specifies the file name
<number>	Specifies the listed number the file appears as
[nostats]	This parameter can be used with [tech_support ap] and [tech_support all]. If the [nostats] option is specified, the technical support file will not have any traffic statistic information.

Examples

The following example creates a tech-support file for Wireless AP, Enterasys Wireless Controller, and log information, which is assigned a default file name. A comment to identify the file is also added.

```
EWC.enterasys.com# tech_support all
Filename (tech_support.06122005.135027):
Comment: Technical support information for MrUser12
Please wait...
Creating tech_support.06122005.135027...
Executing AP commands...
.........................
Executing AC commands...
.....................................................................................
.........................
Executing LOG commands...
Tech_support backup complete.
```

Examples

The following example deletes a tech-support file by name.

```
EWC.enterasys.com# no tech_support tech_ap.tar.gz
Successfully deleted file tech_ap.tar.gz
```

3.24 traceroute

Use the **traceroute** command to perform a traceroute to a specified IP address. Optionally, you can specify the source interface.

Syntax

```
traceroute [source-interface {name <name> | number <id>}] <IP Address>
```

Parameters

source-interface	Keyword indicating that a source interface will be specified.
name <*name*>	Identifies the source interface by name. The names are platform specific. You can use the **show topology** command to display a list of interfaces.
number <*id*>	Identifies the source interface by number. The numbers are platform specific.
<*IP Address*>	Specifies an IP address.

Examples

The following example performs a traceroute to a specified IP Address

```
EWC.enterasys.com# traceroute 68.142.226.40
traceroute to 68.142.226.40 (68.142.226.40), 30 hops max, 38 byte packets
 1  192.168.1.1 (192.168.1.1)  0.801 ms  0.749 ms  0.729 ms
 2  67.69.27.57 (67.69.27.57)  1.898 ms  1.909 ms  1.894 ms
 3  64.230.194.178 (64.230.194.178)  9.660 ms  14.352 ms  11.032 ms
 4  64.230.233.81 (64.230.233.81)  9.666 ms  10.382 ms  9.307 ms
 5  64.230.222.21 (64.230.222.21)  10.266 ms  10.114 ms  10.300 ms
 6  206.108.107.230 (206.108.107.230)  10.169 ms  9.392 ms  10.494 ms
 7  209.58.25.69 (209.58.25.69)  10.458 ms  9.367 ms  10.942 ms
 8  216.6.57.33 (216.6.57.33)  28.928 ms  29.757 ms  30.315 ms
 9  216.6.57.42 (216.6.57.42)  36.011 ms  35.677 ms  34.488 ms
10  63.243.149.110 (63.243.149.110)  38.094 ms  33.761 ms  35.160 ms
11  216.115.96.189 (216.115.96.189)  34.285 ms 216.115.96.173 (216.115.96.173)
40.339 ms 216.115.96.193 (216.115.96.193)  34.594 ms
12 206.190.33.95 (206.190.33.95) 36.994 ms 206.190.33.93 (206.190.33.93) 36.402
ms 206.190.33.89 (206.190.33.89)  32.584 ms
13  68.142.226.40 (68.142.226.40)  36.595 ms  35.023 ms  35.818 ms
```

The following example performs a traceroute, specifying the source interface by number.

```
EWC.enterasys.com# traceroute source-interface number 2 192.168.3.12
traceroute to 192.168.3.12 (192.168.3.12) from 10.1.0.1, 30 hops max, 38 byte pa
ckets
 1  ac_esa_port_0 (10.1.0.1)  3001.190 ms !H  3000.825 ms !H  3000.581 ms !H
```

3.25 upgrade

Use the **upgrade** commands to upgrade the software of the Enterasys Wireless Controller, Operating System, or the Wireless APs.

3.25.1 upgrade ac

Use the **upgrade ac** command to upgrade the controller software. The **upgrade ac** command is accessible from the root context of the CLI.

Syntax

```
upgrade ac <filename|number|ftp> [bckto local|flash [<filename>]|ftp]
```

Parameters

<filename>	Specifies the file name of the new image.
<number>	Specifies an ordinal image number returned by the **[show upgrade]** command
<ftp>	Specifies ftp server on which the upgrade image is uploaded. This ftp server is set by **[upgrade_image_src]** command.
[bckto local]	Backs up the existing operating system of the controller to the local drive. The **[bckto local]** command is supported only on the platforms that support local storage.
[bckto ftp]	Backs up the existing operating system of the controller to the remote FTP server. The FTP server is set by the **upgrade_backup_dest** command.
[bckto flash [<filename>]]	Backs up the existing operating system of the controller to the external flash.

Examples

In the following example, the .gps image file for the C20 was downloaded prior to running the upgrade command.

```
EWC.enterasys.com# upgrade ac AC-MV-07.41.03.0003-1.gps
```

In the following example, the .gps image file for the C20 was downloaded prior to running the upgrade command, and the existing os image is backed up to a remote ftp server.

```
EWC.enterasys.com# upgrade ac AC-MV-07.41.03.0003-1.gps bckto ftp
```

Note: If you use the `bckto ftp` option in the syntax, you must first set the settings of the ftp server, where the existing os image will be backed up, by running the **upgrade_backup_dest** command. For more information, see "3.26, upgrade_backup_dest" on page 3-69.

In the following example, the upgrade image is downloaded from the remote ftp server.

```
EWC.enterasys.com# upgrade ac ftp
```

Note: If you use the `ftp` option in the syntax, you must first specify the details of the ftp server, where the new image is located, by running the **upgrade_image_src** command. For more information, see "3.27, upgrade_image_src" on page 3-69.

In the following example, the upgrade image is downloaded from the remote ftp server and the existing image of the os is backed up to the remote ftp server.

```
EWC.enterasys.com#  upgrade ac ftp bckto ftp
```

Note: If you use the `ftp` and `bckto ftp` options in the syntax, you must first set the settings of the ftp server, where the existing os image will be backed up, by running the **upgrade_backup_dest** command, and then specify the details of the ftp server, where the new image is located, by running the **upgrade_image_src** command. For more information, see "3.26, upgrade_backup_dest" on page 3-69, and "3.27, upgrade_image_src" on page 3-69.

In the following example, the upgrade image is downloaded from the remote ftp server, and the existing image of the os backed up to the flash card.

```
EWC.enterasys.com# upgrade ac ftp bckto flash backupfile-rescue-user.tgz
::::::::::::::::::::::::::::::::::::::::
:: Access Controller Software          ::
:: Application Upgrade / Downgrade     ::
::::::::::::::::::::::::::::::::::::::::
WARNING: Upgrading the controller will disconnect any clients currently using the
system. Following the upgrade, the system will be rebooted.
Do you wish to continue? (y/n) Y
```

Note: If you use the `ftp` option in the syntax, you must first specify the details of the ftp server, where the new image is located, by running the **upgrade_image_src** command. For more information, see "3.27, upgrade_image_src" on page 3-69.

3.25.2 upgrade apup

Use the **upgrade apup** command to upgrade the software of the Wireless AP. The **upgrade apup** command is accessible from the root context of the CLI.

Syntax

```
upgrade apup <platform> <filename|number> ap <ap_serial# ap_serial# ...
ap_serial#>
```

Parameters

<platform>	Specifies the platform of the Wireless AP
<filename>	Specifies the file name of the new image.
<number>	Specifies an ordinal image number returned by the **[show upgrade]|[show osupgrade]** command
<ap_serial#>	Specifies the serial number of the Wireless AP

Examples

The following example upgrades a w788 platform Wireless AP.

```
EWC.enterasys.com# upgrade apup w788 1 ap 0122003999382
```

Caution: Upgrading an AP will disconnect any clients currently using the AP. Following the upgrade, the AP will be rebooted.

3.26 upgrade_backup_dest

Use the **upgrade_backup_dest** command to backup the controller's existing software image on the remote ftp server.

Syntax

```
upgrade_backup_dest <server> <user> <password> <dir> <file>
```

Parameters

<server>	The FTP server where the backup image will be created.
<user>	The user name to access the FTP server.
<password>	The password to access the FTP server.
<dir>	The directory where the new software image is located.
<file>	The file name that you want to assign to the backup image.

Examples

The following example backs up the controller's existing software image on the remote ftp server.

```
EWC.enterasys.com# upgrade_backup_dest 192.168.4.181 administrator abc123 /backup
backupFile.tgz
```

3.27 upgrade_image_src

Use the **upgrade_image_src** command to locate the new software image on the remote server.

Syntax

```
upgrade_image_src <server> <user> <password> <dir> <file>
```

Parameters

<server>	The FTP server on which the new software image is located.
<user>	The user name to access the FTP server.
<password>	The password to access the FTP server
<dir>	The directory where the new software image is located.
<file>	The file name of the software image.

Examples

The following example locates the new software image on the remote server.

```
EWC.enterasys.com# upgrade_image_src 192.168.4.10 test abc123 /ac/rpm/
Build07.41.03.0003 AC-MV-07.41.03.0003-1.gps
```

4

ap Commands

This section describes commands required to manage the basic functions of the Wireless APs on the system. These commands are found in the **ap** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **ap** context:

- access
- blacklist — See blacklist for commands in the **ap:blacklist** context.
- defaults — See defaults for commands in the **ap:defaults** context.
- export_drm
- import_drm
- load-groups — See load-groups for commands in the **ap:load-groups** context.
- maintenance — See maintenance for commands in the **ap:maintenance** context.
- registration — See registration for commands in the **ap:registration** context.
- remove
- search
- serial
- <serial> — See <serial> for commands in the **ap:<serial>** context.

4.1 access

Use the **access** command to modify the registration status of Wireless APs on the system. The **access** command is accessible from the **ap** context of the CLI.

Syntax

```
access <ap_serial> <release|pending|approved|reboot|standalone|
(sensor [force])>
```

Parameters

<ap_serial>	The serial number of the Wireless AP

release | pending | approved | reboot|standalone| sensor [force]	The administrative options for the Wireless AP

Usage

Configuring an 802.11n AP as **standalone** disconnects the AP from the HiPath Wireless Controller and converts the AP to standalone operation mode.

After you convert an 802.11n AP to standalone mode, you can no longer access it using the HiPath Wireless Controller UI or CLI. Instead, you must access AP using the 802.11n AP UI or CLI.

Note: You can convert an 802.11n AP to standalone mode if the AP is local and its status is active. You cannot covert an 802.11n AP to standalone mode if the AP is foreign and its status is inactive. Use the **show ap access** command to identify which APs are active and local.

Examples

The following example modifies the status of an Wireless AP to pending.

```
EWC.enterasys.com:ap# access 0409920201204003 pending
```

The following example reboots the Wireless AP.

```
EWC.enterasys.com:ap# access 0500008043050355 reboot
Rebooting selected AP may result in a localized service interruption. Are you sure
you want to continue(yes/no)?
(yes/no):yes
```

4.2 blacklist

The **blacklist** command moves you into the **blacklist** context, which contains commands to configure a MAC address list. If the MAC address list mode is **black**, the MAC addresses on the list identify clients that are not allowed to associate with the AP (a "blacklist"). If the MAC list mode is **white**, only the clients identified by the MAC addresses on the list are allowed to associate with the AP (a "whitelist"). The **blacklist** command is accessible from the **ap** context of the CLI.

The following commands are available in the **ap:blacklist** context:

- export
- import
- mac
- mac-list-mode

4.2.1 export

Use the **export** command to export the current MAC address list to a file. The **export** command is accessible from the **ap:blacklist** context of the CLI.

Syntax

```
export <server> <user> <dir> <file>
```

Parameters

<server>	Specifies the IP address of the server
<user>	Specifies the username of an account on the server
<dir>	Specifies the directory containing the file
<file>	Specifies the file name

Examples

The following example exports the MAC address list to a file on a server

```
EWC.enterasys.com:ap:blacklist# export 192.168.1.6 mgrey /mgrey/home MAClist.txt
Please input password:
Attempting to upload file...
```

4.2.2 import

Use the **import** command to import a list of MAC addresses for the MAC address list from a file. The **import** command is accessible from the **ap:blacklist** context of the CLI.

Syntax

```
import <server> <user> <dir> <file>
```

Parameters

<server>	Specifies the IP address of the server
<user>	Specifies the username of an account on the server
<dir>	Specifies the directory containing the file
<file>	Specifies the file name

Examples

The following example imports a MAC address list file from a server

```
EWC.enterasys.com:ap:blacklist# import 192.168.1.3 jdoe /jdoe/home MAClist.txt
Please input password:
Attempting to download file...
```

4.2.3 mac

Use the **mac** command to add a new MAC address to the MAC address list. Use the **no** form of the command to remove an address from the MAC address list. The **mac** command is accessible from the **ap:blacklist** context of the CLI.

Syntax

```
mac <MAC Address>
no mac <MAC Address>
```

Parameters

<MAC Address>	Specifies the MAC address to be added to the MAC address list.

Examples

The following example adds a MAC address to the MAC address list.

```
EWC.enterasys.com:ap:blacklist# mac 43:0D:37:5C:8A:12
EWC.enterasys.com:ap:blacklist# show
mac-list-mode black
43:0D:37:5C:8A:12
```

4.2.4 mac-list-mode

Use this command to set the mode of the MAC address list. If the MAC address list mode is **black**, the MAC addresses on the list identify clients that are not allowed to associate with the AP (a "blacklist"). If the MAC list mode is **white**, only the clients identified by the MAC addresses on the list are allowed to associate with the AP (a "whitelist").

Syntax

```
mac-list-mode black|white
```

Parameters

black	Sets the MAC address list as a blacklist, denying clients on the list access to the AP. This is the default.
white	Sets the MAC address list as a whitelist, allowing only clients on the list access to the AP.

Usage

If you change the mode from blacklist to whitelist, all existing MAC addresses on the list will be erased. Use the **show** command to list the current mode and entries in the MAC address list.

Examples

This example shows the system prompt printed when changing from black mode to white mode.

```
EWC.enterasys.com:ap:blacklist# mac-list-mode white
Change address list from whitelist to blacklist or vice versa will erase all
existing address. Are you sure to do it?
(yes/no):no
```

4.3 defaults

Use the **defaults** refers to the **defaults** context, which contains commands to configure the Wireless AP's default settings. The **defaults** command is accessible from the **ap** context of the CLI.

Note: As the Wireless APs discover and register with the controller, they inherit the properties of the default Wireless AP setting. You can modify the default Wireless AP setting either via the Enterasys Wireless Assistant GUI or the CLI.

The following commands are available in the **ap:defaults** context:

- 11n — See 11n for commands in the **ap:defaults:11n** context.
- 4102 — See 4102 for commands in the **ap:defaults:4102** context.
- assign — See assign for commands in the **ap:defaults:assign** context.
- dualband — See dualband for commands in the **ap:defaults:dualband** context.
- learnac
- std — See std for commands in the **ap:defaults:std** context.

4.3.1 11n

The **11n** command refers to context **11n**, which contains commands to configure the default AP settings for the Wireless 802.11n AP (AP3610/AP3620). The **11n** command is accessible from the **ap:defaults** context of the CLI.

The following commands are available in the **ap:defaults:11n** context:

- bcast_disassoc
- client_session
- country
- lbs-status
- led-mode
- lldp
- persistent
- poll_timeout
- radio1 — See radio1 for commands in the **ap:defaults:11n:radio1** context.
- radio2 — See radio2 for commands in the **ap:defaults:11n:radio2** context.
- show

4.3.1.1 bcast_disassoc

Use the **bcast_disassoc** command to enable the Wireless AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. Use the **no** form of the command to disable the feature. The **bcast_disassoc** command is accessible from the **ap:defaults:11n** context of the CLI.

Syntax

```
bcast_disassoc
no bcast_disassoc
```

Parameters

None

Examples

The following disassociates clients from the Wireless AP

```
EWC.enterasys.com:ap:defaults:11n# bcast_disassoc
```

Note: After you have run the **bcast_disassoc** command, you must run the **apply** command to implement the change in broadcast disassociation.

4.3.1.2 client_session

Use the **client_session** command to enable users to maintain client sessions in the event of a poll failure. Use the **no** form of the command to disable the feature. The **client_session** command is accessible from the **ap:defaults:11n** context of the CLI.

Syntax

```
client_session
no client_session
```

Parameters

None

Examples

The following example enables user client sessions

```
EWC.enterasys.com:ap:defaults:11n# client_session
```

Note: After you have run the **client_session** command, you must run the **apply** command to implement the change in client session.

4.3.1.3 country

Use the **country** command to specify the country the Wireless AP resides in. The **country** command is accessible from the **ap:defaults:11n** context of the CLI.

Note: This option is not available for controllers using a single-country license, such as Japan, Thailand, or Israel.

Syntax

```
country <country_name>
```

Parameters

<country_name>	Specifies the name of the country

Examples

The following example sets the name of the country to United States.

```
EWC.enterasys.com:ap:defaults:11n# country United States
```

Note: After you have run the **country** command, you must run the **apply** command to implement the change in country.

4.3.1.4 lbs-status

Use the **lbs-status** command to enable or disable the collection of AeroScout tags for all 802.11n APs. The **lbs-status** command is accessible from the **ap:defaults:11n** context of the CLI.

Syntax

```
lbs-status enable | disable
```

Parameters

enable|disable	Enable or disable the collection of AeroScout tags for the 802.11n APs.

Examples

The following example enables the collection of AeroScout tags for the 802.11n APs.

```
EWC.enterasys.com:ap:defaults:11n# lbs-status enable
```

4.3.1.5 led-mode

Use the **led-mode** command to configure the behavior of the LEDs on the Wireless AP. The **led-mode** command is accessible from the **ap:defaults:11n** context of the CLI.

Syntax

```
led-mode normal | off
```

Parameters

normal	Identifies the AP status at all times while the AP is powered on.
off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.

Examples

The following example turns off LED activity:

```
EWC.enterasys.com:ap:defaults:11n# led-mode off
```

4.3.1.6 lldp

Use the **lldp** command to enable the broadcast of the LLDP protocol by a Wireless AP. Use the **no** form of the command to disable LLDP. The **lldp** command is accessible from the **ap:defaults:11n** context of the CLI.

Syntax

```
lldp <Announcement Interval> <Announcement Delay>
no lldp
```

Parameters

<Announcement Interval>	Specifies the scheduled frequency, measured in seconds, in which the Wireless AP advertises its information by sending a new LLDP packet. Range is 5 to 32768.

<Announcement Delay>	Specifies the delay, measured in seconds, between successive LLDP frame transmissions that is initiated by a value/status change in the LLDP local systems MIB. Range is 1 to 1/4 x Announcement Interval value.

Examples

The following example enables LLDP for the default Wireless AP configuration with an announcement interval of 30 seconds, and an announcement delay of 2.

```
EWC.enterasys.com:ap:defaults:11n# lldp 30 2
```

If SNMP is enabled to publish on the Enterasys Wireless Controller and you enable LLDP, the following message is displayed:

```
WARNING: SNMP is set to publish. How Do you wish to continue?
(C) Cancel
(P) Proceed
(O) Disable SNMP publishing and proceed
```

Type one of the following:

- **C** – Cancels the LLDP configuration and returns to the AP context.
- **P** – Enables LLDP and maintains SNMP running
- **O** – Enables LLDP and disables SNMP publishing

4.3.1.7 persistent

Use the **persistent** command to enable mode persistence. Use the **no** form of the command to disable the feature. The **persistent** command is accessible from the **ap:defaults:11n** context of the CLI.

Syntax

```
persistent
no persistent
```

Parameters

None

Examples

The following example enables mode persistence.

```
EWC.enterasys.com:ap:defaults:11n# persistent
```

Note: After you have run the **persistent** command, you must run the **apply** command to implement the change in mode persistence value.

4.3.1.8 poll_timeout

Use the **poll_timeout** command to set the amount of time the Wireless AP will wait for a response from the Enterasys Wireless Controller before rebooting. The **poll_timeout** command is accessible from the **ap:defaults:11n** context of the CLI.

Syntax

```
poll_timeout <value>
```

Note: The acceptable range for poll_timeout value is from 3 to 600.

Parameters

<value>	Specifies the amount of time, in seconds, to wait for a response from the Enterasys Wireless Controller before rebooting.

Examples

The following example sets the poll timeout to 20 seconds

```
EWC.enterasys.com:ap:defaults:11n# poll_timeout 20
```

Note: After you have run the **poll_timeout** command, you must run the **apply** command to implement the change in poll timeout value.

4.3.1.9 radio1

The **radio1** command refers to the **radio1** context, which contains commands to configure Radio 1 of the Wireless AP. The **radio1** command is accessible from the **ap:defaults:11n** context of the CLI.

The following commands are available in the **ap:defaults:11n:radio1** context:

- admin-mode
- antsel
- atpc
- beaconp
- dcs — See dcs for commands in the **ap:defaults:11n:radio1:dcs** context.
- domain
- dtim
- frag
- max-distance
- minbrate
- mode
- n_addba_support
- n_aggr_mpdu
- n_aggr_mpdu_max
- n_aggr_mpdu_max_subframes

- n_aggr_msdu
- n_aggr_msdu_max
- n_chlbonding
- n_chlwidth
- n_guardinterval
- n_pbthreshold
- n_pmode
- n_poffset
- n_ptype
- rts
- tx_adjust_power
- tx_max_power
- tx_min_power

4.3.1.9.1 admin-mode

Use this comment to configure the administration status for the radio. The **admin-mode** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
admin-mode off|on
```

Parameters

off	Clear the administrative status.
on	Set the administrative status. On is the default.

Examples

```
EWC.enterasys.com:ap:defaults:11n:radio1# admin-mode on
```

4.3.1.9.2 antsel

Use the **antsel** command to configure the antenna, or antenna combination, you want to use for Radio 1.The **antsel** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
antsel (left | middle | right | left-middle | left-right |  middle-right | left-middle-right)
```

Parameters

left	Specifies the use of the left antenna on the Wireless 802.11n AP.
middle	Specifies the use of the middle antenna on the Wireless 802.11n AP.
right	Specifies the use of the right antenna on the Wireless 802.11n AP.

left-middle	Specifies the use of the left-middle antenna combination on the Wireless 802.11n AP.
left-right	Specifies the use of the left-right antenna combination on the Wireless 802.11n AP.
middle-right	Specifies the use of the middle-right antenna combination on the Wireless 802.11n AP.
left-middle-right	Specifies the use of the left-middle-right antenna combination on the Wireless 802.11n AP.

Examples

The following example depicts Radio 1of the Wireless 802.11n AP configured to use the left-middle-right antenna combination.

```
EWC.enterasys.com:ap:defaults:11n:radio1# antsel left-middle-right
```

Note: After you have run the **antsel** command, you must run the **apply** command to implement the change.

4.3.1.9.3 atpc

Use the **atpc** command to enable Auto Tx Power Ctrl (ATPC). Use the **no** form of the command to disable the feature. The **atpc** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
atpc
no atpc [maintain_power]
```

Parameters

[maintain_power]	When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established.

Examples

The following example disables atpc on Radio 1.

```
EWC.enterasys.com:ap:defaults:11n:radio1# no atpc maintain_power
```

Note: After you have run the **atpc** command, you must run the **apply** command to implement the change.

4.3.1.9.4 beaconp

Use the **beaconp** command to set time units between beacon transmissions. The **beaconp** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
beaconp <value>
```

Parameters

<value>	Specifies the number of time units (milliseconds) between beacon transmissions. The acceptable range for beaconp value is from 50 to 1000 milliseconds.

Examples

The following example sets the time between successive beacons to 70 ms on Radio 1.

```
EWC.enterasys.com:ap:defaults:11n:radio1# beaconp 70
```

Note: After you have run the **beaconp** command, you must run the **apply** command to implement the change.

4.3.1.9.5 dcs

The **dcs** command refers to the **dcs** context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The **dcs** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Note: Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

The following commands are available in the **ap:defaults:11n:radio1:dcs** context:

- channel_plan
- mode
- noise_threshold
- occupancy_threshold
- radio_channels
- update_period

4.3.1.9.5.1 channel_plan

Use the **channel_plan** command to customize the channel plan for the Wireless AP's Radio 1. The **channel_plan** command is accessible from the **ap:defaults:11n:radio1:dcs** context of the CLI.

Syntax

```
channel_plan <all-non-dfs|all|channel[, channel]>
```

Note: The parameters available in the **channel_plan** command are determined by the setting of the **mode** command in the **ap:defaults:11n:radio1** context.

Parameters

all-non-dfs	Radio 1 uses all non-DFS channels.
all	Radio 1 uses all channels
channel[, channel]	Radio 1 uses the channels that are listed, separated by commas.

Examples

The following example shows the channel plan for Radio 1 is configured to include all non-DFS channels.

```
EWC.enterasys.com:ap:defaults:11n:radio1:dcs# channel_plan all-non-dfs
```

The following example shows that the channel plan for radio 1is customized to include channels 1, 2 and 3..

```
EWC.enterasys.com:ap:defaults:11n:radio1:dcs# channel_plan 1, 2, 3
```

4.3.1.9.5.2 mode

Use the **mode** command to set the **DCS** mode. The **mode** command is accessible from the **ap:defaults:11n:radio1:dcs** context of the CLI.

Syntax

```
mode <off|monitor|active>
```

Parameters

off	Disables DCS
monitor	Monitors the noise and interference on the current channel
active	Enables DCS

Note: In monitor mode, DCS generates an alarm and does not change the channel if the noise and interference levels on the current channel exceed beyond their thresholds. In active mode, DCS changes the channel if the noise and interference levels on the current channel exceed beyond their thresholds.

Examples

The following example sets DCS to active mode.

```
EWC.enterasys.com:ap:defaults:11n:radio1:dcs# mode active
```

4.3.1.9.5.3 noise_threshold

Use the **noise_threshold** command to set the DCS noise threshold. The **noise_threshold** command is accessible from the **ap:defaults:11n:radio1:dcs** context of the CLI.

Syntax

```
noise_threshold <thrshold>
```

Parameters

<thrshold>	Specifies the DCS noise threshold in dBm. The DCS noise threshold must be in the -95 to -50 range. ACS will scan for a new operating channel for the Wireless AP if the threshold is exceeded.

Examples

The following example sets the noise threshold to -45 dBm.

```
EWC.enterasys.com:ap:defaults:11n:radio1:dcs# noise_threshold -45
```

4.3.1.9.5.4 occupancy_threshold

Use the **occupancy_threshold** command to set the DCS Channel Occupancy Threshold. The **occupancy_threshold** command is accessible from the **ap:defaults:11n:radio1:dcs** context of the CLI.

Syntax

```
occupancy_threshold <thrshold>
```

Parameters

thrshold	Specifies the DCS Occupancy Threshold as a percentage. The DCS Occupancy Threshold must be in the 10 to 100 range.

Examples

The following example sets the DCS Channel Occupancy Threshold to 10 per cent.

```
EWC.enterasys.com:ap:defaults:11n:radio1:dcs# occupancy_threshold 10
```

4.3.1.9.5.5 radio_channels

Use the **radio_channels** command to display the list of available radio channels for auto channel selection (ACS). The **radio_channels** command is accessible from the **ap:defaults:11n:radio1:dcs** context of the CLI.

Syntax

```
radio_channels
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:defaults:std:radio1:dcs# radio_channels
Available radio channels:
        36: 5180 MHz
        40: 5200 MHz
        44: 5220 MHz
        48: 5240 MHz
        52: 5260 MHz
        56: 5280 MHz
        60: 5300 MHz
        64: 5320 MHz
        100: 5500 MHz
        104: 5520 MHz
```

```
108: 5540 MHz
112: 5560 MHz
116: 5580 MHz
120: 5600 MHz
124: 5620 MHz
128: 5640 MHz
132: 5660 MHz
136: 5680 MHz
140: 5700 MHz
149: 5745 MHz
153: 5765 MHz
157: 5785 MHz
161: 5805 MHz
165: 5825 MHz
```

4.3.1.9.5.6 update_period

Use the **update_period** command to set the DCS update period, during which the Wireless AP averages the DCS noise threshold and DCS channel occupancy threshold measurements. If either one of these thresholds is exceeded, the Wireless AP will trigger ACS. The **update_period** command is accessible from the **ap:defaults:11n:radio1:dcs** context of the CLI.

Syntax

```
update_period <period>
```

Parameters

<period>	Specifies the time period, measured in minutes, during which the Wireless AP averages the DCS noise threshold and DCS channel occupancy threshold measurements. If either one of these thresholds is exceeded, then the Wireless AP will trigger ACS Range is 1 to 15 minutes.

Examples

The following example sets the DCS update period to 2 minutes.

```
EWC.enterasys.com:ap:defaults:11n:
1:dcs# update_period 2
```

4.3.1.9.6 domain

Use the **domain** command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The **domain** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
domain <domain_name>
```

Note: The maximum length of the domain string is 16 characters.

Parameters

<domain_name>	Specifies the group name of APs that cooperate in managing RF channels.

Examples

The following example assigns the name **test** to the group of APs that cooperate in managing RF channels and transmission power levels.

```
EWC.enterasys.com:ap:defaults:11n:radio1# domain test
```

4.3.1.9.7 dtim

Use the **dtim** command to set the Delivery Traffic Indication Message (DTIM) period. The **dtim** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
dtim <value>
```

Note: The acceptable range for the dtim value is from 1 to 255 beacon intervals.

Parameters

<value>	Specifies the DTIM period in beacons

Examples

The following example sets the Delivery Traffic Indication Message period to 2 beacons.

```
EWC.enterasys.com:ap:defaults:11n:radio1# dtim 2
```

4.3.1.9.8 frag

Use the **frag** command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold will be fragmented into packets that are less than or equal to this limit. The **frag** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
frag <value>
```

Parameters

<value>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery. Range is 256 to 2346.

Examples

The following example sets the fragmentation threshold to 1500

```
EWC.enterasys.com:ap:defaults:11n:radio1# frag 1500
```

4.3.1.9.9 max-distance

Use the **max-distance** command to set the maximum link distance, in meters, between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. If the link distance between APs is greater than the default value of 100 meters, configure the maximum distance up to 15000 meters so that the software increases the timeout value proportionally with the distance between APs. The **max-distance** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Note: Do not change the default setting for the radio that provides service to 802.11 clients only.

Syntax

```
max-distance <value>
```

Parameters

value	Specifies the maximum distance between APs in meters. The default is 100 meters. You can enter a value from 100 to 15000 meters.

Examples

The following example sets the maximum distance between APs to 1500 meters.

```
EWC.enterasys.com:ap:defaults:11n:radio1# max-distance 1500
```

4.3.1.9.10 minbrate

Use this command to configure the minimum basic data rate for radio 1. The **minbrate** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
minbrate <min-rate>
```

Parameters

Valid values for <min-rate> depend on the radio mode and are expressed as Mbps:

Radio Mode	Minimum Basic Rate Range per Mode
a	6, 12, 24
an	6, 12, 24
n-strict	6, 12, 24, MCS0 – MCS7

Usage

The minimum basic rate must be lower than or equat to the configured maximum basic data rate and maximum data rate that clients can operate at while associated with the AP.

Examples

This example sets the mode for radio 1 to a, then sets the minimum basic data rate to 12 Mbps.

```
EWC.enterasys.com:ap:defaults:11n:radio1# mode a
EWC.enterasys.com:ap:defaults:11n:radio1# minbrate 12
```

4.3.1.9.11 mode

Use the **mode** command to set the radio options for Radio 1. Use the **no** form of the command to disable Radio 1. The **mode** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
mode a|an|n-strict
```

Note: Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Parameters

a	Enable only 802.11a mode of Radio 1.
an	Enable both the 802.11a mode and the 802.11n mode of Radio 1.
n-strict	Enable the 802.11a mode of Radio 1 with 802.11n strict capability.

Examples

```
EWC.enterasys.com:ap:defaults:11n:radio1# mode a
```

4.3.1.9.12 n_addba_support

Use the **n_addba_support** command to enable the ADDBA support. Use the **no** command to disable the feature. The **n_addba_support** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_addba_support
no n_addba_support
```

Parameters

None

Examples

The following example enables the ADDBA support.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_addba_support
```

4.3.1.9.13 n_aggr_mpdu

Use the **n_aggr_mpdu** command to enable the use of aggregate MPDU's. Use the **no** command to disable this feature. The **n_aggr_mpdu** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_aggr_mpdu
no n_aggr_mpdu
```

Parameters

None

Examples

The following example disables MPDU.

```
EWC.enterasys.com:ap:defaults:11n:radio1# no n_aggr_mpdu
```

4.3.1.9.14 n_aggr_mpdu_max

Use the **n_aggr_mpdu_max** command to specify the maximum length of the aggregate MPDU. The **n_aggr_mpdu_max** is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_aggr_mpdu_max <1024-65535>
```

Parameters

<1024-65535>	The maximum size in bytes for an aggregate MPDU.The range of values allowed is 1024 to 65535.

Examples

The following example sets the maximum length of the aggregate MPDU to 5000 bytes.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_aggr_mpdu_max 5000
```

4.3.1.9.15 n_aggr_mpdu_max_subframes

Use the **n_aggr_mpdu_max_subframes** command to specify the maximum number of subframes that may be contained in an aggregate MPDU. The **n_aggr_mpdu_max_subframes** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_aggr_mpdu_max_subframes <2-64>
```

Parameters

<2-64>	The maximum number of subframes allowed in an aggregate MPDU. The acceptable range of values is from 2 to 64.

Examples

The following example sets the maximum number of subframes to 50.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_aggr_mpdu_max_subframes 50
```

4.3.1.9.16 n_aggr_msdu

Use the **n_aggr_msdu** command to enable the use of aggregate MSDUs. Use the **no** command to disable the use of aggregate MSDUs. The **n_aggr_msdu** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_aggr_msdu
no n_aggr_msdu
```

Parameters

None

Examples

The following example disables the aggregate MSDU.

```
EWC.enterasys.com:ap:defaults:11n:radio1# no n_aggr_msdu
```

4.3.1.9.17 n_aggr_msdu_max

Use the **n_aggr_msdu_max** command to specify the maximum length of a A-MSDU. The **n_aggr_msdu_max** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_aggr_msdu_max <2290-4096>
```

Parameters

<2290-4096>	The maximum size of bytes of a A-MSDU. The range of values allowed is 2290 to 4096.

Examples

The following example sets the maximum length of the aggregate MSDU to 3000 bytes.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_aggr_msdu_max 3000
```

4.3.1.9.18 n_chlbonding

Use the **n_chlbonding** command to specify the channel bonding type — up or down. The **n_chlbonding** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_chlbonding (up|down)
```

Parameters

up	The primary channel (20MHz) is bonded with an extension channel that is 20MHz above (bonding up) the primary channel.
down	The primary channel (20MHz) is bonded with an extension channel that is 20MHz below (bonding down) the primary channel.

Examples

The following example sets the channel bonding type as up.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_chlbonding up
```

Note: Depending on the channel you have selected, you may be prevented from bonding up or down. For more information, see the Enterasys Wireless Controller, *Access Points and Convergence Software User Guide*.

4.3.1.9.19 n_chlwidth

Use the **n_chlwidth** command to specify the 802.11n channel width — 20 MHz or 40 MHz. This command only has effect when the mode is set to enable 802.11n. The **n_chlwidth** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_chlwidth (20|40|auto)
```

Parameters

20	Specifies the channel width as 20 MHz
40	Specifies the channel width as 40 MHz
auto	Specifies that the AP will automatically select the channel width depending upon how busy the extension channel is. The extension channel threshold is set via the n_pbthreshold command.

Examples

The following example sets the channel width to 40 MHz.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_chlwidth 40
```

4.3.1.9.20 n_guardinterval

Use the **n_guardinterval** command to specify the guard interval — short or long. The **n_guardinterval** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_guardinterval short|long
```

Parameters

short	Specifies a short guard interval
long	Specifies a short guard interval

Examples

The following example sets the long guard interval.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_guardinterval long
```

4.3.1.9.21 n_pbthreshold

Use the **n_pbthreshold** command to specify the extension channel threshold. This value is used to determine which channel width to use when the **n_chlwidth** is set to **auto**. The **n_pbthreshold** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_pbthreshold <0-100>
```

Parameters

<0-100>	Specifies the extension channel threshold value as a percentage.

Examples

The following example sets the extension channel threshold value to 60 per cent.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_pbthreshold 60
```

4.3.1.9.22 n_pmode

Use the **n_pmode** command to enable the protection on the primary channel. Use the **no** command to disable protection. The **n_pmode** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_pmode
no n_pmode
```

Parameters

None

Examples

The following example enables the protection mode

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_pmode
```

4.3.1.9.23 n_poffset

Use the **n_poffset** command to set the 40MHz Protection Channel Offset. The **n_poffset** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_poffset 20|25
```

Parameters

20	Specifies a 20 MHz channel offset
25	Specifies a 25 MHz channel offset

Examples

The following example sets the protection channel offset to 20 MHz.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_poffset 20
```

4.3.1.9.24 n_ptype

Use the **n_ptype** command to specify the 40 MHz protection type — whether CTS, RTS or none. The **n_ptype** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
n_ptype {none|cts only|rts cts}
```

Parameters

none	No 40 MHz protection type is enabled.
cts only	Specifies Clear to Send (CTS) protection type.
rts cts	Specifies Receive to Send (RTS) / Clear to Send (CTS) protection type.

Examples

The following example sets the clear to send (CTS) protection type.

```
EWC.enterasys.com:ap:defaults:11n:radio1# n_ptype cts only
```

4.3.1.9.25 rts

Use the **rts** command to specify the size of the Request to Send (RTS) threshold. The **rts** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Syntax

```
rts <value>
```

Note: The acceptable value for the rts value is 1 to 2346.

Parameters

<value>	Specifies the Request to Send packet size threshold.

Examples

The following example sets the RTS packet size to 256

```
EWC.enterasys.com:ap:defaults:11n:radio1# rts 256
```

4.3.1.9.26 tx_adjust_power

Use the **tx_adjust_power** command to specify an offset to the Tx power level, which is used to adjust the ATPC power levels from the calculated value. The **tx_adjust_power** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Note: The **tx_adjust_power** command is available only when Auto Tx Power Ctrl (ATPC) is enabled.

Syntax

```
tx_adjust_power <value>
```

Parameters

<value>	Specifies the value in dBm

Examples

The following example specifies the Tx power level to 0 dBm.

```
EWC.enterasys.com:ap:defaults:11n:radio1# tx_adjust_power 0
```

4.3.1.9.27 tx_max_power

Use the **tx_max_power** command to set the maximum Tx power level. The **tx_max_power** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Note: The **tx_max_power** is a maximum level when ATPC is enabled, and a fixed level when it ATPC is disabled.

Syntax

```
tx_max_power <value>
```

Parameters

<value>	Specifies the maximum Tx power level.

Examples

The following example sets the maximum Tx power level to 18 dBm.

```
EWC.enterasys.com:ap:defaults:11n:radio1# tx_max_power 18
```

4.3.1.9.28 tx_min_power

Use the **tx_min_power** command to specify the minimum Tx power level. The **tx_min_power** command is accessible from the **ap:defaults:11n:radio1** context of the CLI.

Note: The tx_min_power is available only when Auto Tx Power Ctrl (ATPC) is enabled.

Syntax

```
tx_min_power <value>
```

Parameters

<value>	Specifies the value in dBm

Examples

The following example specifies the minimum Tx power level to 8 dBm.

```
EWC.enterasys.com:ap:defaults:11n:radio1# tx_min_power 8
```

4.3.1.10 radio2

The **radio2** command refers to the **radio2** context, which contains commands to configure Radio 2 of the Wireless AP. The **radio2** command is accessible from the **ap:defaults:11n** context of the CLI.

The following commands are available in the **ap:defaults:11n:radio2** context:

- admin-mode
- antsel
- atpc
- beaconp
- dcs — See dcs for commands in the **ap:defaults:11n:radio2:dcs** context.
- domain
- dtim
- frag
- max-distance
- minbrate
- mode
- n_addba_support
- n_aggr_mpdu
- n_aggr_mpdu_max
- n_aggr_mpdu_max_subframes

- n_aggr_msdu
- n_aggr_msdu_max
- n_chlbonding
- n_chlwidth
- n_guardinterval
- n_pbthreshold
- n_pmode
- n_poffset
- n_ptype
- pmode
- prate
- preamble
- ptype
- rts
- tx_max_power

4.3.1.10.1 admin-mode

Use this comment to configure the administration status for the radio. The **admin-mode** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
admin-mode off|on
```

Parameters

off	Clear the administrative status.
on	Set the administrative status. On is the default.

Examples

```
EWC.enterasys.com:ap:defaults:11n:radio2# admin-mode on
```

4.3.1.10.2 antsel

Use the **antsel** command to configure the antenna, or antenna combination, you want to use for Radio 2. The **antsel** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
antsel (left | middle | right | left-middle | left-right |  middle-right | left-middle-right)
```

Parameters

left	Specifies the use of the left antenna on the Wireless 802.11n AP.

middle	Specifies the use of the middle antenna on the Wireless 802.11n AP.
right	Specifies the use of the right antenna on the Wireless 802.11n AP.
left-middle	Specifies the use of the left-middle antenna combination on the Wireless 802.11n AP.
left-right	Specifies the use of the left-right antenna combination on the Wireless 802.11n AP.
middle-right	Specifies the use of the middle-right antenna combination on the Wireless 802.11n AP.
left-middle-right	Specifies the use of the left-middle-right antenna combination on the Wireless 802.11n AP.

Examples

The following example depicts Radio 2 of the Wireless 802.11n AP configured to use the left-middle-right antenna combination.

```
EWC.enterasys.com:ap:defaults:11n:radio2# antsel left-middle-right
```

4.3.1.10.3 atpc

Use the **atpc** command to enable Auto Tx Power Ctrl (ATPC). Use the **no** form of the command to disable the ATPC feature. The **atpc** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
atpc
no atpc [maintain_power]
```

Parameters

[maintain_power]	When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established.

Examples

The following example disables atpc on Radio 1.

```
EWC.enterasys.com:ap:defaults:11n:radio2# no atpc maintain_power
```

4.3.1.10.4 beaconp

Use the **beaconp** command to set time units between beacon transmissions. The **beaconp** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
beaconp <value>
```

Parameters

<value>	Specifies the number of time units (milliseconds) between beacon transmissions. The acceptable range for beaconp value is from 50 to 1000 milliseconds.

Examples

The following example sets the time between successive beacons to 70 ms on Radio 2.

```
EWC.enterasys.com:ap:defaults:11n:radio2# beaconp 70
```

4.3.1.10.5 dcs

The **dcs** command refers to the **dcs** context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The **dcs** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Note: Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

The following commands are available in the **ap:defaults:11n:radio2:dcs** context:

- channel_plan
- mode
- radio_channels

4.3.1.10.5.1 channel_plan

Use the **channel_plan** command to customize the channel plan for the Wireless AP's Radio 2. The **channel_plan** command is accessible from the **ap:defaults:11n:radio2:dcs** context of the CLI.

Syntax

```
channel_plan <auto|3-channel|4-channel|channel[, channel]>
```

Note: The parameters available in the **channel_plan** command are determined by the setting of the **mode** command in the **ap:defaults:11n:radio2** context.

Parameters

auto	Radio 2 uses 3 channels for countries supporting 11 channels and 4 channels for countries supporting 13 channels.
3-channel	Radio 2 uses 3 channels.
4-channel	Radio 2 uses 4 channels.
channel [,channel]	Radio 2 uses the channels that are listed, separated by commas.

Example

The following example shows that the channel plan for radio 2 is customized to include channels 1, 2 and 3.

```
EWC.enterasys.com:ap:defaults:11n:radio2:dcs# channel_plan 1, 2, 3
```

4.3.1.10.5.2 mode

Use the **mode** command to set the **DCS** mode. The **mode** command is accessible from the **ap:defaults:11n:radio2:dcs** context of the CLI.

Syntax

```
mode <off|monitor|active>
```

Parameters

off	Disables DCS
monitor	Monitors the noise and interference on the current channel
active	Enables DCS

Note: In monitor mode, DCS generates an alarm and does not change the channel if the noise and interference levels on the current channel exceed beyond their thresholds. In active mode, DCS changes the channel if the noise and interference levels on the current channel exceed beyond their thresholds.

Examples

The following example sets DCS to active mode.

```
EWC.enterasys.com:ap:defaults:11n:radio2:dcs# mode active
```

4.3.1.10.5.3 radio_channels

Use the **radio_channels** command to display the list of available radio channels for auto channel selection (ACS). The **radio_channels** command is accessible from the **ap:defaults:11n:radio2:dcs** context of the CLI.

Syntax

```
radio_channels
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:defaults:11n:radio1:dcs# radio_channels
Available radio channels:
        1: 2412 MHz
        2: 2417 MHz
        3: 2422 MHz
        4: 2427 MHz
        5: 2432 MHz
        6: 2437 MHz
        7: 2442 MHz
        8: 2447 MHz
        9: 2452 MHz
        10: 2457 MHz
```

```
11: 2462 MHz
```

4.3.1.10.6 domain

Use the **domain** command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The **domain** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
domain <domain_name>
```

Note: The maximum length of the domain string is 15 characters.

Parameters

<domain_name>	Specifies the group name of APs that cooperate in managing RF channels.

Examples

The following example assigns the name **test** to the group of APs that cooperate in managing RF channels and transmission power levels.

```
EWC.enterasys.com:ap:defaults:11n:radio2# domain test
```

4.3.1.10.7 dtim

Use the **dtim** command to set the Delivery Traffic Indication Message (DTIM) period. The **dtim** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
dtim <value>
```

Note: The acceptable range for the dtim value is from 1 to 255 beacon intervals.

Parameters

<value>	Specifies the DTIM period in beacons

Examples

The following example sets the Delivery Traffic Indication Message period to 2 beacons.

```
EWC.enterasys.com:ap:defaults:11n:radio2# dtim 2
```

4.3.1.10.8 frag

Use the **frag** command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold will be fragmented into packets

that are less than or equal to this limit. The **frag** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
frag <value>
```

Parameters

<value>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery.

Examples

The following example sets the fragmentation threshold to 1500

```
EWC.enterasys.com:ap:defaults:11n:radio2# frag 1500
```

4.3.1.10.9 max-distance

Use the **max-distance** command to set the maximum link distance, in meters, between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. If the link distance between APs is greater than the default value of 100 meters, configure the maximum distance up to 15,000 meters so that the software increases the timeout value proportionally with the distance between APs. The **max-distance** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Note: Do not change the default setting for any radio that is not participating in a Mesh or WDS.

Syntax

```
max-distance <value>
```

Parameters

<value>	Specifies the maximum distance between APs in meters. The default is 100 meters. You can enter a value from 100 to 15000 meters.

Examples

The following example sets the maximum distance between APs to 1500 meters.

```
EWC.enterasys.com:ap:defaults:11n:radio2# max-distance 1500
```

4.3.1.10.10 minbrate

Use this command to configure the minimum basic data rate for radio 2. The **minbrate** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
minbrate <min-rate>
```

Parameters

Valid values for <min-rate> depend on the radio mode and are expressed as Mbps:

Radio Mode	Minimum Basic Rate Range per Mode
b	1, 2, 5.5, 11
g	6, 12, 24
gn	6, 12, 24
n-strict	6, 12, 24, MCS0 – MCS7
bg	1, 2, 5.5, 11
bgn	1, 2, 5.5, 11

Usage

The minimum basic rate must be lower than or equat to the configured maximum basic data rate and maximum data rate that clients can operate at while associated with the AP.

Examples

This example sets the mode for radio 2 to g, then sets the minimum basic data rate to 12 Mbps.

```
EWC.enterasys.com:ap:defaults:11n:radio2# mode g
EWC.enterasys.com:ap:defaults:11n:radio2# minbrate 12
```

4.3.1.10.11 mode

Use the **mode** command to set the radio options for Radio 2. Use the **no** form of the command to disable Radio 2. The **mode** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
mode b|g|gn|n-strict|bg|bgn
```

Note: Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Parameters

b	Enables the 802.11b-only mode of Radio 2. If enabled, the AP will use only 11b (CCK) rates with all associated clients.
g	Enables the 802.11g-only mode of Radio 2. The AP will use 11g-only (OFDM) rates with all associated clients.
gn	Enables both the 802.11g mode and the 802.11n mode of **Radio 2**. If selected, the AP will use 11n and 11g-specific (OFDM) rates with all of the associated clients. The AP will not transmit or receive 11b rates.
n-strict	Enables the 802.11n-strict mode of **Radio 2**. If selected, the AP will use 11n and (optionally) 11g rates with all of the associated clients. The AP will not transmit or receive 11b rates..
bg	Enables both the 802.11g mode and the 802.11b mode of Radio 2. If enabled, the AP will use 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients. The AP will not transmit or receive 11n rates.

bgn	Enable b/g/n modes of Radio 2. If enabled, the AP will use all available 11b, 11g, and 11n rates.

Examples

The following example enables only 802.11b mode of Radio 2.

```
EWC.enterasys.com:ap:defaults:11n:radio2# mode b
```

The following example enables both 802.11b mode and 802.11g mode of Radio 2.

```
EWC.enterasys.com:ap:defaults:11n:radio2# mode bg
```

4.3.1.10.12 n_addba_support

Use the **n_addba_support** command to enable the ADDBA support. Use the **no** command to disable the feature. The **n_addba_support** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_addba_support
no n_addba_support
```

Parameters

None

Examples

The following example enables the ADDBA support.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_addba_support
```

4.3.1.10.13 n_aggr_mpdu

Use the **n_aggr_mpdu** command to enable the use of aggregate MPDUs. Use the **no** command to disable this feature. The **n_aggr_mpdu** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_aggr_mpdu
no n_aggr_mpdu
```

Parameters

None

Examples

The following example disables MPDU.

```
EWC.enterasys.com:ap:defaults:11n:radio2# no n_aggr_mpdu
```

4.3.1.10.14 n_aggr_mpdu_max

Use the **n_aggr_mpdu_max** command to specify the maximum length of the aggregate MPDU. The **n_aggr_mpdu_max** is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_aggr_mpdu_max <1024-65535>
```

Parameters

<1024-65535>	The maximum size in bytes for an aggregate MPDU.The range of values allowed is 1024 to 65535.

Examples

The following example sets the maximum length of the aggregate MPDU to 5000 bytes.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_aggr_mpdu_max 5000
```

4.3.1.10.15 n_aggr_mpdu_max_subframes

Use the **n_aggr_mpdu_max_subframes** command to specify the maximum number of subframes that may be contained in an aggregate MPDU. The **n_aggr_mpdu_max_subframes** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_aggr_mpdu_max_subframes <2-64>
```

Parameters

<2-64>	The maximum number of subframes allowed in an aggregate MPDU. The acceptable range of values is from 2 to 64.

Examples

The following example sets the maximum number of subframes to 50.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_aggr_mpdu_max_subframes 50
```

4.3.1.10.16 n_aggr_msdu

Use the **n_aggr_msdu** command to enable the use of aggregate MSDUs. Use the **no** command to disable the use of aggregate MSDUs. The **n_aggr_msdu** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_aggr_msdu
no n_aggr_msdu
```

Parameters

None

Examples

The following example disables the aggregate MSDU.

```
EWC.enterasys.com:ap:defaults:11n:radio2# no n_aggr_msdu
```

4.3.1.10.17 n_aggr_msdu_max

Use the **n_aggr_msdu_max** command to specify the maximum length of an A-MSDU. The **n_aggr_msdu_max** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_aggr_msdu_max <2290-4096>
```

Parameters

<2290-4096>	The maximum size of bytes of a A-MSDU. The range of values allowed is 2290 to 4096.

Examples

The following example sets the maximum length of the aggregate MSDU to 3000 bytes.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_aggr_msdu_max 3000
```

4.3.1.10.18 n_chlbonding

Use the **n_chlbonding** command to specify the channel bonding type — up or down. The **n_chlbonding** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_chlbonding (up|down)
```

Parameters

up	The primary channel (20MHz) is bonded with an extension channel that is 20MHz above (bonding up) the primary channel.
down	The primary channel (20MHz) is bonded with an extension channel that is 20MHz below (bonding down) the primary channel.

Examples

The following example sets the channel bonding type as up.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_chlbonding up
```

Note: Depending on the channel you have selected, you may be prevented from bonding up or down. For more information, see the *Enterasys Wireless Controller, Access Points and Convergence Software User Guide.*

4.3.1.10.19 n_chlwidth

Use the **n_chlwidth** command to specify the 802.11n channel width — 20 MHz or 40 MHz. This command only has affect when the mode is set to enable 802.11n. The **n_chlwidth** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_chlwidth (20|40|auto)
```

Parameters

20	Specifies the channel width as 20 MHz
40	Specifies the channel width as 40 MHz
auto	Specifies that the AP will automatically select the channel width depending upon how busy the extension channel is. The extension channel threshold is set via the n_pbthreshold command.

Examples

The following example sets the channel width to 40 MHz.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_chlwidth 40
```

4.3.1.10.20 n_guardinterval

Use the **n_guardinterval** command to specify the guard interval — short or long. The **n_guardinterval** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_guardinterval short|long
```

Parameters

short	Specifies a short guard interval
long	Specifies a short guard interval

Examples

The following example sets the long guard interval.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_guardinterval long
```

4.3.1.10.21 n_pbthreshold

Use the **n_pbthreshold** command to specify the extension channel threshold. This value is used to determine which channel width to use when the **n_chlwidth** is set to **auto**. The **n_pbthreshold** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_pbthreshold <0-100>
```

Parameters

<0-100>	Specifies the extension channel threshold value as a percentage.

Examples

The following example sets the extension channel threshold value to 60 per cent.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_pbthreshold 60
```

4.3.1.10.22 n_pmode

Use the **n_pmode** command to enable the protection on the primary channel. Use the **no** command to disable protection. The **n_pmode** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_pmode
no n_pmode
```

Parameters

None

Examples

The following example enables the protection mode

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_pmode
```

4.3.1.10.23 n_poffset

Use the **n_poffset** command to set the 40MHz Protection Channel Offset. The **n_poffset** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_poffset 20|25
```

Parameters

20	Specifies a 20 MHz channel offset
25	Specifies a 25 MHz channel offset

Examples

The following example sets the protection channel offset to 20 MHz.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_poffset 20
```

4.3.1.10.24 n_ptype

Use the **n_ptype** command to specify the 40 MHz protection type — whether CTS, RTS or none. The **n_ptype** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
n_ptype {none|cts only|rts cts}
```

Parameters

none	No 40 MHz protection type is enabled.
cts only	Specifies Clear to Send (CTS) protection type.
rts cts	Specifies Receive to Send (RTS) / Clear to Send (CTS) protection type.

Examples

The following example sets the clear to send (CTS) protection type.

```
EWC.enterasys.com:ap:defaults:11n:radio2# n_ptype cts only
```

4.3.1.10.25 pmode

Use the **pmode** command to configure the Protection Mode, which will protect 802.11g client transmissions from interruption by 802.11b clients. The **pmode** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
pmode (none|auto|always)
```

Parameters

none	Deactivates Protection Mode
auto	Indicates that Protection Mode will be used only when 802.11b clients or Wireless APs are detected
always	Indicates that Protection Mode will remain active at all times

Caution: Only use **none** if the Wireless AP will NOT be servicing 802.11b clients, and there are no 802.11b clients or Wireless APs sharing the same air space.

Examples

The following example configures the Wireless AP to use Protection Mode at all times

```
EWC.enterasys.com:ap:defaults:11n:radio2# pmode always
```

4.3.1.10.26 prate

Use the **prate** command to adjust the Protection Rate. The **prate** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
prate (1|2|5.5|11)
```

Parameters

1|2|5.5|11	Specifies the Protection Rate in Mbps

Examples

The following example adjusts the Protection Rate to 5.5 Mbps

```
EWC.enterasys.com:ap:defaults:11n:radio2# prate 5.5
```

4.3.1.10.27 preamble

Use the **preamble** command to set the preamble type. The **preamble** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
preamble (short|long|auto)
```

Parameters

short	Specifies short preambles
long	Specifies long preambles
auto	Indicates that preamble types will be automatically selected by the Wireless AP

Note: For preambles set to “auto” the Wireless AP will use short preambles, unless clients using the original 802.11 standard are detected.

Examples

The following example enables the long option for the preamble type

```
EWC.enterasys.com:ap:defaults:11n:radio2# preamble long
```

4.3.1.10.28 ptype

Use the **ptype** command to select the Protection Type. The **ptype** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
ptype (cts only|rts cts)
```

Parameters

cts only	Specifies the Clear to Send (CTS) type.
rts cts	Specifies the Request to Send (RTS) and Clear to Send (CTS) ypes

Examples

The following example sets the protection type to CTS

```
EWC.enterasys.com:ap:defaults:11n:radio2# ptype cts only
```

4.3.1.10.29 rts

Use the **rts** command to specify the size of the Request to Send (RTS) threshold. The **rts** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Syntax

```
rts <value>
```

Note: The acceptable value for the rts value is 1 to 2346.

Parameters

<value>	Specifies the Request to Send packet size threshold.

Examples

The following example sets the RTS packet size to 256

```
EWC.enterasys.com:ap:defaults:11n:radio2# rts 256
```

4.3.1.10.30 tx_max_power

Use the **tx_max_power** command to set the maximum Tx power level. The **tx_max_power** command is accessible from the **ap:defaults:11n:radio2** context of the CLI.

Note: The **tx_max_power** is a maximum level when ATPC is enabled, and a fixed level when it ATPC is disabled.

Syntax

```
tx_max_power <value>
```

Parameters

<value>	Specifies the maximum Tx power level.

Examples

The following example sets the maximum Tx power level to 18 dBm.

```
EWC.enterasys.com:ap:defaults:11n:radio2# tx_max_power 18
```

4.3.1.11 show

Use the **show** command to display 802.11n AP information. The **show** command is accessible from the **ap:defaults:11n** context of the CLI.

Syntax

```
show
```

Parameters

None.

Examples

The following example displays 802.11n AP information.

```
EWC.enterasys.com:ap:defaults:11n# show
telnet
poll_timeout 15
client_session
no persistent
no bcast_disassoc
country United States
led-mode normal
lbs-status enabled
```

4.3.2 4102

The **4102** command refers to context **4102**, which contains commands to configure the default AP settings for the Wireless AP 4102. The **4102** command is accessible from the **ap:defaults** context of the CLI.

The following commands are available in the **ap:defaults:4102** context:

- bcast_disassoc
- client_session
- country
- led-mode
- lldp
- persistent
- poll_timeout
- radio1 — See radio1 for commands in the **ap:defaults:4102:radio1** context.
- radio2 — See radio2 for commands in the **ap:defaults:4102:radio2** context.
- telnet

4.3.2.1 bcast_disassoc

Use the **bcast_disassoc** command to enable the Wireless AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. Use the **no** form of the

command to disable the feature. The **bcast_disassoc** command is accessible from the **ap:defaults:4102** context of the CLI.

Syntax

```
bcast_disassoc
no bcast_disassoc
```

Parameters

None

Examples

The following disassociates clients from the Wireless AP

```
EWC.enterasys.com:ap:defaults:4102# bcast_disassoc
```

Note: After you have run the **bcast_disassoc** command, you must run the **apply** command to implement the change in broadcast disassociation.

4.3.2.2 client_session

Use the **client_session** command to enable users to maintain client sessions in the event of a poll failure. Use the **no** form of the command to disable the feature. The **client_session** command is accessible from the **ap:defaults:4102** context of the CLI.

Syntax

```
client_session
no client_session
```

Parameters

None

Examples

The following example enables user client sessions

```
EWC.enterasys.com:ap:defaults:4102# client_session
```

Note: After you have run the **client_session** command, you must run the **apply** command to implement the change in client session.

4.3.2.3 country

Use the **country** command to specify the country the Wireless AP resides in. The **country** command is accessible from the **ap:defaults:4102** context of the CLI.

Syntax

```
country <country_name>
```

Parameters

<country_name>	Specifies the name of the country

Examples

The following example sets the name of the country to United States.

```
EWC.enterasys.com:ap:defaults:4102# country United States
```

Note: After you have run the **country** command, you must run the **apply** command to implement the change in country.

4.3.2.4 led-mode

Use the **led-mode** command to configure the behavior of the LEDs on the Wireless AP. The **led-mode** command is accessible from the **ap:defaults:4102** context of the CLI.

Syntax

```
led-mode off | normal
```

Parameters

off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.
normal	Identifies the AP status during the registration process during power on and boot process.

Examples

The following example turns off LED activity:

```
EWC.enterasys.com:ap:defaults:4102# led-mode off
```

4.3.2.5 lldp

Use the **lldp** command to enable the broadcast of the LLDP protocol by a Wireless AP. Use the **no** form of the command to disable LLDP. The **lldp** command is accessible from the **ap:defaults:4102** context of the CLI.

Syntax

```
lldp <Announcement Interval> <Announcement Delay>
no lldp
```

Parameters

<Announcement Interval>	Specifies the scheduled frequency, measured in seconds, in which the Wireless AP advertises its information by sending a new LLDP packet.
<Announcement Delay>	Specifies the delay, measured in seconds, between successive LLDP frame transmissions that is initiated by a value/status change in the LLDP local systems MIB.

Examples

The following example enables LLDP for the default Wireless AP configuration with an announcement interval of 30 seconds, and an announcement delay of 2.

```
EWC.enterasys.com:ap:defaults:4102# lldp 30 2
```

If SNMP is enabled to publish on the Enterasys Wireless Controller and you enable LLDP, the following message is displayed:

```
WARNING: SNMP is set to publish. How Do you wish to continue?
(C) Cancel
(P) Proceed
(O) Disable SNMP publishing and proceed
```

Type one of the following:

- **C** – Cancels the LLDP configuration and returns to the AP context.
- **P** – Enables LLDP and maintains SNMP running
- **O** – Enables LLDP and disables SNMP publishing

4.3.2.6 persistent

Use the **persistent** command to enable mode persistence. Use the **no** form of the command to disable the feature. The **persistent** command is accessible from the **ap:defaults:4102** context of the CLI.

Syntax

```
persistent
no persistent
```

Parameters

None

Examples

The following example enables mode persistence.

```
EWC.enterasys.com:ap:defaults:4102# persistent
```

Note: After you have run the **persistent** command, you must run the **apply** command to implement the change in mode persistence value.

4.3.2.7 poll_timeout

Use the **poll_timeout** command to set the amount of time the Wireless AP will wait for a response time from the Enterasys Wireless Controller before rebooting. The **poll_timeout** command is accessible from the **ap:defaults:4102** context of the CLI.

Syntax

```
poll_timeout <value>
```

Note: The acceptable range for poll_timeout value is from 3 to 600.

Parameters

<value>	Specifies the amount of time, in seconds, to wait for a response from the Enterasys Wireless Controller before rebooting.

Examples

The following example sets the poll timeout to 20 seconds

```
EWC.enterasys.com:ap:defaults:4102# poll_timeout 20
```

Note: After you have run the **poll_timeout** command, you must run the **apply** command to implement the change in poll timeout value.

4.3.2.8 radio1

The **radio1** command refers to the **radio1** context, which contains commands to configure Radio 1 of the Wireless AP. The **radio1** command is accessible from the **ap:defaults:4102** context of the CLI.

The following commands are available in the **ap:defaults:4102:radio1** context:

- admin-mode
- atpc
- beaconp
- dcs — See dcs for commands in the **ap:defaults:4102:radio1:dcs** context.
- divrx
- divtx
- domain
- dtim
- frag
- hwretries
- maxbrate
- maxoprate
- max-distance
- minbrate
- mode
- rts
- tx_adjust_power
- tx_max_power
- tx_min_power

4.3.2.8.1 admin-mode

Use this comment to configure the administration status for the radio. The **admin-mode** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
admin-mode off|on
```

Parameters

off	Clear the administrative status.
on	Set the administrative status. On is the default.

Examples

```
EWC.enterasys.com:ap:defaults:4102:radio1# admin-mode on
```

4.3.2.8.2 atpc

Use the **atpc** command to enable Auto Tx Power Ctrl (ATPC). Use the **no** form of the command to disable the feature. The **atpc** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
atpc
no atpc [maintain_power]
```

Parameters

[maintain_power]	When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established.

Examples

The following example disables atpc on Radio 1.

```
EWC.enterasys.com:ap:defaults:4102:radio1# no atpc maintain_power
```

4.3.2.8.3 beaconp

Use the **beaconp** command to set time units between beacon transmissions. The **beaconp** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
beaconp <value>
```

Parameters

<value>	Specifies the number of time units (milliseconds) between beacon transmissions. The acceptable range for beaconp value is from 50 to 1000 milliseconds.

Examples

The following example sets the time between successive beacons to 70 ms on Radio 1.

```
EWC.enterasys.com:ap:defaults:4102:radio1# beaconp 70
```

4.3.2.8.4 dcs

The **dcs** command refers to the **dcs** context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The **dcs** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Note: Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

The following commands are available in the **ap:defaults:4102:radio1:dcs** context:

- channel_plan
- mode
- radio_channels

4.3.2.8.4.1 channel_plan

Use the **channel_plan** command to customize the channel plan for the Wireless AP's Radio 1. The **channel_plan** command is accessible from the **ap:defaults:4102:radio1:dcs** context of the CLI.

Syntax

```
channel_plan <all-non-dfs|all|channel[, channel]>
```

Note: The parameters available in the **channel_plan** command are determined by the setting of the **mode** command in the **ap:defaults:4102:radio1** context.

Parameters

all-non-dfs	Radio 1 uses all non-DFS channels.
all	Radio 1 uses all channels
channel[, channel]	Radio 1 uses the channels that are listed, separated by commas.

Examples

The following example shows the channel plan for Radio 1 is configured to include all non-DFS channels.

```
EWC.enterasys.com:ap:defaults:4102:radio1:dcs# channel_plan all-non-dfs
```

The following example shows that the channel plan for radio 1 is customized to include channels 1, 2 and 3.

```
EWC.enterasys.com:ap:defaults:4102:radio1:dcs# channel_plan 1, 2, 3
```

4.3.2.8.4.2 mode

Use the **mode** command to set the **DCS** mode. The **mode** command is accessible from the **ap:defaults:4102:radio1:dcs** context of the CLI.

Syntax

```
mode <off|monitor|active>
```

Parameters

off	Disables DCS
monitor	Monitors the noise and interference on the current channel
active	Enables DCS

Note: In monitor mode, DCS generates an alarm and does not change the channel if the noise and interference levels on the current channel exceed beyond their thresholds. In active mode, DCS changes the channel if the noise and interference levels on the current channel exceed beyond their thresholds.

Examples

The following example sets DCS to active mode.

```
EWC.enterasys.com:ap:defaults:4102:radio1:dcs# mode active
```

4.3.2.8.4.3 radio_channels

Use the **radio_channels** command to display the list of available radio channels for auto channel selection (ACS). The **radio_channels** command is accessible from the **ap:defaults:4102:radio1:dcs** context of the CLI.

Syntax

```
radio_channels
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:defaults:4102:radio1:dcs# radio_channels
Available radio channels:
        36: 5180 MHz
        40: 5200 MHz
        44: 5220 MHz
        48: 5240 MHz
        52: 5260 MHz
        56: 5280 MHz
        60: 5300 MHz
        64: 5320 MHz
        100: 5500 MHz
        104: 5520 MHz
```

```
108: 5540 MHz
112: 5560 MHz
116: 5580 MHz
120: 5600 MHz
124: 5620 MHz
128: 5640 MHz
132: 5660 MHz
136: 5680 MHz
140: 5700 MHz
149: 5745 MHz
153: 5765 MHz
157: 5785 MHz
161: 5805 MHz
165: 5825 MHz
```

4.3.2.8.5 divrx

Use the **divrx** command to select the best signal from the pair of diversity antennas for the reception of packets from client devices. Select **best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The **divrx** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
divrx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:4102:radio1# divrx right
```

4.3.2.8.6 divtx

Use the **divtx** command to select the best signal from the pair of diversity antennas for the transmission of packets to client devices. Select **best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The **divtx** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
divtx <alternate|left|right>
```

Parameters

alternative | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:4102:radio1# divtx right
```

4.3.2.8.7 domain

Use the **domain** command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The **domain** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
domain <domain_name>
```

Note: The maximum length of the domain string is 15 characters.

Parameters

<domain_name>	Specifies the group name of APs that cooperate in managing RF channels.

Examples

The following example assigns the name **test** to the group of APs that cooperate in managing RF channels and transmission power levels.

```
EWC.enterasys.com:ap:defaults:4102:radio1# domain domain_test
```

4.3.2.8.8 dtim

Use the **dtim** command to set the Delivery Traffic Indication Message (DTIM) period. The **dtim** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
dtim <value>
```

Note: The acceptable range for the dtim value is from 1 to 255 beacon intervals.

Parameters

<value>	Specifies the DTIM period in beacons

Examples

The following example sets the Delivery Traffic Indication Message period to 2 beacons.

```
EWC.enterasys.com:ap:defaults:4102:radio1# dtim 2
```

4.3.2.8.9 frag

Use the **frag** command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold will be fragmented into packets that are less than or equal to this limit. The **frag** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
frag <value>
```

Parameters

<value>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery. Range is 256 to 2346.

Examples

The following example sets the fragmentation threshold to 1500

```
EWC.enterasys.com:ap:defaults:4102:radio1# frag 1500
```

4.3.2.8.10 hwretries

Use the **hwretries** command to set the number of retries for background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and turbo voice transmission queue. The **hwretries** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
hwretries (BK|BE|VI|VO|TVO) <value>
```

Parameters

BK	Specifies the number of retries for the Background transmission queue.
BE	Specifies the number of retries for the Best Effort transmission queue.
VI	Specifies the number of retries for the Video transmission queue.
VO	Specifies the number of retries for the Voice transmission queue.
TVO	Specifies the number of retries for the Turbo Voice transmission queue.

Examples

The following example sets the retry values for the background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and the turbo voice transmission queue as 1, 2, 3, 4, 5 respectively.

Note: You can set each parameter — background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue and turbo voice transmission queue — to any value from 0 to a. (0 means adaptive, a means 10. 1 through 9 mean 1 through 9.)

```
EWC.enterasys.com:ap:defaults:4102:radio1# hwretries 12345
```

4.3.2.8.11 maxbrate

Use the **maxbrate** command to configure the maximum basic rate. The **maxbrate** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
maxbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps. The maximum basic rate choices adjust automatically to be higher or equal to the minimum basic rate.

Parameters

<value>	Specifies the maximum basic rate value in Mbps

Examples

The following example configures the maximum basic rate to 24 Mbps

```
EWC.enterasys.com:ap:defaults:4102:radio1# maxbrate 24
```

4.3.2.8.12 maxoprate

Use the **maxoprate** command to set the maximum operational rate. The **maxoprate** is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Note: Available operational rate values (in Mbps) for Radio **1** are: 6, 9, 12, 18, 24, 36, 48, and 54.

Syntax

```
maxoprate <value>
```

Parameters

<value>	Specifies the maximum operational rate value in Mbps

Examples

The following example sets the maximum operational rate to 24Mbps

```
EWC.enterasys.com:ap:defaults:4102:radio1# maxoprate 24
```

4.3.2.8.13 max-distance

Use the **max-distance** command to set the maximum link distance, in meters, between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. If the link distance between APs is greater than the default value of 100 meters, configure the maximum distance up to 15,000 meters so that the software increases the timeout value proportionally with the distance

between APs. The **max-distance** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Note: Do not change the default setting for any radio that is not participating in a Mesh or WDS.

Syntax

```
max-distance <value>
```

Parameters

<value>	Specifies the maximum distance between APs in meters. The default is 100 meters. You can enter a value from 100 to 15000 meters.

Examples

The following example sets the maximum distance between APs to 1500 meters.

```
EWC.enterasys.com:ap:defaults:4102:radio1# max-distance 1500
```

4.3.2.8.14 minbrate

Use the **minbrate** command to configure the minimum basic rate. The **minbrate** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
minbrate <value>
```

Parameters

<value>	Specifies the minimum basic rate value in Mbps. Valid values are 6, 12, and 24.

Examples

The following example configures the minimum basic rate to 6 Mbps

```
EWC.enterasys.com:ap:defaults:4102:radio1# minbrate 6
```

4.3.2.8.15 mode

Use the **mode** command to set the radio options for Radio 1. Use the **no** form of the command to disable Radio 1. The **mode** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Syntax

```
mode <a>
```

Note: Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Parameters

a	Enable 802.11a mode of Radio 1.

Examples

The following example enables only 802.11a mode of Radio 1.

```
EWC.enterasys.com:ap:defaults:4102:radio1# mode a
```

4.3.2.8.16 rts

Use the **rts** command to specify the size of the Request to Send (RTS) threshold. The **rts** command is accessible from the **ap:defaults:4102:radio1** context of the CLI

Syntax

```
rts <value>
```

Note: The acceptable value for rts value is from 1 to 2346.

Parameters

<value>	Specifies the Request to Send packet size threshold.

Examples

The following example sets the RTS packet size to 256

```
EWC.enterasys.com:ap:defaults:4102:radio1# rts 256
```

4.3.2.8.17 tx_adjust_power

Use the **tx_adjust_power** command to specify an offset to the Tx power level, which is used to adjust the ATPC power levels from the calculated value. The **tx_adjust_power** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Note: The **tx_adjust_power** command is available only when Auto Tx Power Ctrl (ATPC) is enabled.

Syntax

```
tx_adjust_power <value>
```

Parameters

<value>	Specifies the value in dBm

Examples

The following example specifies the Tx power level to 0 dBm.

```
EWC.enterasys.com:ap:defaults:4102:radio1# tx_adjust_power 0
```

4.3.2.8.18 tx_max_power

Use the **tx_max_power** command to set the maximum Tx power level. The **tx_max_power** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Note: The **tx_max_power** is a maximum level when ATPC is enabled, and a fixed level when it ATPC is disabled.

Syntax

```
tx_max_power <value>
```

Parameters

<value>	Specifies the maximum Tx power level.

Examples

The following example sets the maximum Tx power level to 18 dBm.

```
EWC.enterasys.com:ap:defaults:4102:radio1# tx_max_power 18
```

4.3.2.8.19 tx_min_power

Use the **tx_min_power** command to specify the minimum Tx power level. The **tx_min_power** command is accessible from the **ap:defaults:4102:radio1** context of the CLI.

Note: The tx_min_power is available only when Auto Tx Power Ctrl (ATPC) is enabled.

Syntax

```
tx_min_power <value>
```

Parameters

value	Specifies the value in dBm

Examples

The following example specifies the minimum Tx power level to 8 dBm.

```
EWC.enterasys.com:ap:defaults:4102:radio1# tx_min_power 8
```

4.3.2.9 radio2

The **radio2** command refers to the **radio2** context, which contains commands to configure Radio 2 of the Wireless AP. The **radio2** command is accessible from the **ap:defaults:4102** context of the CLI.

The following commands are available in the **ap:defaults:4102:radio2** context:

- admin-mode
- atpc
- beaconp
- dcs — See dcs for commands in the **ap:defaults:4102:radio2:dcs** context.

- divrx
- divtx
- domain
- dtim
- frag
- hwretries
- maxbrate
- max-distance
- maxoprate
- minbrate
- mode
- pmode
- prate
- preamble
- ptype
- rts
- tx_max_power

4.3.2.9.1 admin-mode

Use this comment to configure the administration status for the radio. The **admin-mode** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
admin-mode off|on
```

Parameters

off	Clear the administrative status.
on	Set the administrative status. On is the default.

Examples

```
EWC.enterasys.com:ap:defaults:4102:radio2# admin-mode on
```

4.3.2.9.2 atpc

Use the **atpc** command to enable Auto Tx Power Ctrl (ATPC). Use the **no** form of the command to disable the feature. The **atpc** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
atpc
no atpc [maintain_power]
```

Parameters

[maintain_power]	When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established.

Examples

The following example disables atpc on Radio 2.

```
EWC.enterasys.com:ap:defaults:4102:radio2# no atpc maintain_power
```

4.3.2.9.3 beaconp

Use the **beaconp** command to set time units between beacon transmissions. The **beaconp** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
beaconp <value>
```

Parameters

<value>	Specifies the number of time units (milliseconds) between beacon transmissions. The acceptable range for beaconp value is from 50 to 1000 milliseconds.

Examples

The following example sets the time between successive beacons to 70 ms on Radio 2.

```
EWC.enterasys.com:ap:defaults:4102:radio2# beaconp 70
```

4.3.2.9.4 dcs

The **dcs** command refers to the **dcs** context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The **dcs** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Note: Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

The following commands are available in the **ap:defaults:4102:radio2:dcs** context:

- channel_plan
- mode
- radio_channels

4.3.2.9.4.1 channel_plan

Use the **channel_plan** command to customize the channel plan for the Wireless AP's radio 2. The **channel_plan** command is accessible from the **ap:defaults:4102:radio2:dcs** context of the CLI.

Syntax

```
channel_plan <auto|3-channel|4-channel|channel[, channel]>
```

Note: The parameters available in the **channel_plan** command are determined by the setting of the **mode** command in the **ap:defaults:4102:radio2** context.

Parameters

auto	Radio 2 uses 3 channels for countries supporting 11 channels and 4 channels for countries supporting 13 channels
3-channel	Radio 2 uses 3 channels
4-channel	Radio 2 uses 4 channels
channel [, channel]	Radio 2 uses the channels that are listed, separated by commas

Example

The following example shows that the channel plan for radio 2 is customized to include the following channels: 1, 2 and 3.

```
EWC.enterasys.com:ap:defaults:4102:radio2:dcs# channel_plan 1, 2, 3
```

4.3.2.9.4.2 mode

Use the **mode** command to set the **DCS** mode. The **mode** command is accessible from the **ap:defaults:4102:radio2:dcs** context of the CLI.

Syntax

```
mode <off|monitor|active>
```

Parameters

off	Disables DCS
monitor	Monitors the noise and interference on the current channel
active	Enables

Note: In monitor mode, DCS generates an alarm and does not change the channel if the noise and interference levels on the current channel exceed beyond their thresholds. In active mode, DCS changes the channel if the noise and interference levels on the current channel exceed beyond their thresholds.

Examples

The following example sets DCS to active mode.

```
EWC.enterasys.com:ap:defaults:4102:radio2:dcs# mode active
```

4.3.2.9.4.3 radio_channels

Use the **radio_channels** command to display the list of available radio channels for auto channel selection (ACS). The **radio_channels** command is accessible from the **ap:defaults:4102:radio2:dcs** context of the CLI.

Syntax

```
radio_channels
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:defaults:4102:radio2:dcs# radio_channels
Available radio channels:
        1: 2412 MHz
        2: 2417 MHz
        3: 2422 MHz
        4: 2427 MHz
        5: 2432 MHz
        6: 2437 MHz
        7: 2442 MHz
        8: 2447 MHz
        9: 2452 MHz
        10: 2457 MHz
        11: 2462 MHz
        12: 2467 MHz
        13: 2472 MHz
        14: 2477 MHz
```

4.3.2.9.5 divrx

Use the **divrx** command to select the best signal from the pair of diversity antennas for the reception of packets from client devices. Select **best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The **divrx** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
divrx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:4102:radio2# divrx right
```

4.3.2.9.6 divtx

Use the **divtx** command to select the best signal from the pair of diversity antennas for the transmission of packets to client devices. Select **alternate** for the best signal from both antennas, or **left** or **right** to choose either of the two diversity antennas. The **divtx** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
divtx (alternate|left|right)
```

Parameters

alternate | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:4102:radio2# divtx right
```

4.3.2.9.7 domain

Use the **domain** command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The **domain** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
domain <domain_name>
```

Note: The maximum length of the domain string is 15 characters.

Parameters

<domain_name>	Specifies the group name of APs that cooperate in managing RF channels.

Examples

The following example assigns the name **test** to the group of APs that cooperate in managing RF channels and transmission power levels.

```
EWC.enterasys.com:ap:defaults:4102:radio2# domain test
```

4.3.2.9.8 dtim

Use the **dtim** command to set the Delivery Traffic Indication Message (DTIM) period. The **dtim** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
dtim <value>
```

Note: The acceptable range for the dtim value is from 1 to 255 beacon intervals.

Parameters

<value>	Specifies the DTIM period in beacons

Examples

The following example sets the Delivery Traffic Indication Message period to 2 beacons.

```
EWC.enterasys.com:ap:defaults:4102:radio2# dtim 2
```

4.3.2.9.9 frag

Use the **frag** command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold will be fragmented into packets that are less than or equal to this limit. The **frag** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
frag <value>
```

Parameters

<value>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery.

Examples

The following example sets the fragmentation threshold to 1500

```
EWC.enterasys.com:ap:defaults:4102:radio2# frag 1500
```

4.3.2.9.10 hwretries

Use the **hwretries** command to set the number of retries for background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and turbo voice transmission queue. The **hwretries** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
hwretries (BK|BE|VI|VO|TVO) <value>
```

Parameters

BK	Specifies the number of retries for the Background transmission queue.
BE	Specifies the number of retries for the Best Effort transmission queue.
VI	Specifies the number of retries for the Video transmission queue.
VO	Specifies the number of retries for the Voice transmission queue.
TVO	Specifies the number of retries for the Turbo Voice transmission queue.

Examples

The following example sets the retry values for the background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and the turbo voice transmission queue as 1, 2, 3, 4, 5 respectively.

Note: You can set each parameter — background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue and turbo voice transmission queue — to any value from 0 to 10 (0 means adaptive).

```
EWC.enterasys.com:ap:defaults:4102:radio2# hwretries 12345
```

4.3.2.9.11 maxbrate

Use the **maxbrate** command to configure the maximum basic rate. The **maxbrate** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
maxbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps. The maximum basic rate choices adjust automatically to be higher or equal to the minimum basic rate.

Parameters

<value>	Specifies the maximum basic rate value in Mbps

Examples

The following example configures the maximum basic rate to 24 Mbps

```
EWC.enterasys.com:ap:defaults:4102:radio2# maxbrate 24
```

4.3.2.9.12 max-distance

Use the **max-distance** command to set the maximum link distance, in meters, between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. If the link distance between APs is greater than the default value of 100 meters, configure the maximum distance up to 15,000 meters so that the software increases the timeout value proportionally with the distance between APs. The **max-distance** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Note: Do not change the default setting for any radio that is not participating in a Mesh or WDS.

Syntax

```
max-distance <value>
```

Parameters

<value>	Specifies the maximum distance between APs in meters. The default is 100 meters. You can enter a value from 100 to 15000 meters.

Examples

The following example sets the maximum distance between APs to 1500 meters.

```
EWC.enterasys.com:ap:defaults:4102:radio2# max-distance 1500
```

4.3.2.9.13 maxoprate

Use the **maxoprate** command to set the maximum operational rate. The **maxoprate** is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Note: Available operational rate values (in Mbps) for Radio 2 are: 6, 9, 12, 18, 24, 36, 48, and 54.

Syntax

```
maxoprate <value>
```

Parameters

<value>	Specifies the maximum operational rate value in Mbps

Examples

The following example sets the maximum operational rate to 24Mbps

```
EWC.enterasys.com:ap:defaults:4102:radio2# maxoprate 24
```

4.3.2.9.14 minbrate

Use the **minbrate** command to configure the minimum basic rate. The **minbrate** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
minbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps.

Parameters

<value>	Specifies the minimum basic rate value in Mbps

Examples

The following example configures the minimum basic rate to 6 Mbps

```
EWC.enterasys.com:ap:defaults:4102:radio2# minbrate 6
```

4.3.2.9.15 mode

Use the **mode** command to set the radio options for Radio 2. Use the **no** form of the command to disable Radio 2. The **mode** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
mode <b|g|bg>
```

Note: Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Parameters

b	Enables the 802.11b-only mode of Radio 2. If enabled, the AP will use only 11b (CCK) rates with all associated clients.
g	Enables the 802.11g-only mode of Radio 2. The AP will use 11g-only (OFDM) rates with all associated clients.
bg	Enables both the 802.11g mode and the 802.11b mode of Radio 2. If enabled, the AP will use 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients.

Examples

The following example enables only 802.11b mode of Radio 2.

```
EWC.enterasys.com:ap:defaults:4102:radio2# mode b
```

4.3.2.9.16 pmode

Use the **pmode** command to configure the Protection Mode, which will protect 802.11g client transmissions from interruption by 802.11b clients. The **pmode** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
pmode (none|auto|always)
```

Parameters

none	Deactivates Protection Mode
auto	Indicates that Protection Mode will be used only when 802.11b clients or Wireless APs are detected
always	Indicates that Protection Mode will remain active at all times

Caution: Only use **none** if the Wireless AP will NOT be servicing 802.11b clients, and there are no 802.11b clients or Wireless APs sharing the same air space.

Examples

The following example configures the Wireless AP to use Protection Mode at all times

```
EWC.enterasys.com:ap:defaults:4102:radio2# pmode always
```

4.3.2.9.17 prate

Use the **prate** command to adjust the Protection Rate. The **prate** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
prate (1|2|5.5|11)
```

Parameters

1|2|5.5|11	Specifies the Protection Rate in Mbps

Examples

The following example adjusts the Protection Rate to 5.5 Mbps

```
EWC.enterasys.com:ap:defaults:4102:radio2# prate 5.5
```

4.3.2.9.18 preamble

Use the **preamble** command to set the preamble type. The **preamble** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
preamble (short|long|auto)
```

Parameters

short	Specifies short preambles
long	Specifies long preambles
auto	Indicates that preamble types will be automatically selected by the Wireless AP

Note: For preambles set to auto, the Wireless AP will use short preambles, unless clients using the original 802.11 standard are detected.

Examples

The following example enables the long option for the preamble type

```
EWC.enterasys.com:ap:defaults:4102:radio2# preamble long
```

4.3.2.9.19 ptype

Use the **ptype** command to select the Protection Type. The **ptype** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Syntax

```
ptype (cts only|rts cts)
```

Parameters

cts only	Specifies the Clear to Send (CTS) type
rts cts	Specifies the Request to Send (RTS) and Clear to Send (CTS) types

Examples

The following example sets the protection type to CTS

```
EWC.enterasys.com:ap:defaults:4102:radio2# ptype cts only
```

4.3.2.9.20 rts

Use the **rts** command to specify the size of the Request to Send (RTS) threshold. The **rts** command is accessible from the **ap:defaults:4102:radio2** context of the CLI

Syntax

```
rts <value>
```

Note: The acceptable value for rts value is from 1 to 2346.

Parameters

<value>	Specifies the Request to Send packet size threshold.

Examples

The following example sets the RTS packet size to 256

```
EWC.enterasys.com:ap:defaults:4102:radio2# rts 256
```

4.3.2.9.21 tx_max_power

Use the **tx_max_power** command to set the maximum Tx power level. The **tx_max_power** command is accessible from the **ap:defaults:4102:radio2** context of the CLI.

Note: The **tx_max_power** is a maximum level when ATPC is enabled, and a fixed level when it ATPC is disabled.

Syntax

```
tx_max_power <value>
```

Parameters

<value>	Specifies the maximum Tx power level.

Examples

The following example sets the maximum Tx power level to 18 dBm.

```
EWC.enterasys.com:ap:defaults:4102:radio2# tx_max_power 18
```

4.3.2.10 telnet

Use the **telnet** command to enable telnet access to the Wireless AP. Use the **no** form of the command to disable it. The **telnet** command is accessible from the **ap:defaults:4102** context of the CLI

Syntax

```
telnet
no telnet
```

Parameters

None

Examples

The following example enables telnet access to the Wireless AP

```
EWC.enterasys.com:ap:defaults:4102# telnet
```

Note: After you have run the **telnet** command, you must run the **apply** command to implement the change.

4.3.3 assign

The **assign** command refers to context **assign**, which contains the **wlans-list** command. The **assign** command is accessible from the **ap:defaults** context of the CLI.

4.3.3.1 wlans-list

Use the **wlans-list** command to assign the Radio 1 and Radio2 to the WLANS. Use the **no** command to disable the radios from the WLANS. The **wlans-list** command is accessible from the **ap:defaults:assign** context of the CLI.

Syntax

```
wlans-list <wlans-name> <radio1|radio2>
no vnslist
```

Parameters

<wlans-name>	The name of the WLANS
<radio1>	5GHz radio
<radio2>	2.4GHz radio

Examples

The following example assigns Radio 1 to CNL-209 WLANS.

```
EWC.enterasys.com:ap:defaults:assign# wlans-list CNL-209 radio1
```

Note: After you have run the **wlans-list** command, you must run the **apply** command to implement the changes in radio assignments.

4.3.4 dualband

Use the **dualband** command to configure Wireless AP default configuration for Wireless Outdoor APs. Use **no** form of the command to disable this feature. The dualband command is available from the **ap:defaults** context of the CLI.

The following commands are available in the **ap:defaults:dualband** context:

- bcast_disassoc
- client_session

- country
- led-mode
- lldp
- persistent
- poll_timeout
- radio1 — See radio1 for commands in the **ap:defaults:dualband:radio1** context.
- radio2 — See radio2 for commands in the **ap:defaults:dualband:radio2** context.
- telnet

4.3.4.1 bcast_disassoc

Use the **bcast_disassoc** command to enable the Wireless AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. Use the **no** form of the command to disable the feature. The **bcast_disassoc** command is accessible from the **ap:defaults:dualband** context of the CLI.

Syntax

```
bcast_disassoc
no bcast_disassoc
```

Parameters

None

Examples

The following disassociates clients from the Wireless AP

```
EWC.enterasys.com:ap:defaults:dualband# bcast_disassoc
```

Note: After you have run the **bcast_disassoc** command, you must run the **apply** command to implement the change in broadcast disassociation.

4.3.4.2 client_session

Use the **client_session** command to enable users to maintain client sessions in the event of a poll failure. Use the **no** form of the command to disable the feature. The **client_session** command is accessible from the **ap:defaults:dualband** context of the CLI.

Syntax

```
client_session
no client_session
```

Parameters

None

Examples

The following example enables user client sessions

```
EWC.enterasys.com:ap:defaults:dualband# client_session
```

Note: After you have run the **client_session** command, you must run the **apply** command to implement the change in client session.

4.3.4.3 country

Use the **country** command to specify the country the Wireless AP resides in. The **country** command is accessible from the **ap:defaults:dualband** context of the CLI.

Syntax

```
country <country_name>
```

Parameters

<country_name>	Specifies the name of the country

Examples

The following example sets the name of the country to United States.

```
EWC.enterasys.com:ap:defaults:dualband# country United States
```

Note: After you have run the **country** command, you must run the **apply** command to implement the change in country.

4.3.4.4 led-mode

Use the **led-mode** command to configure the behavior of the LEDs on the Wireless AP. The **led-mode** command is accessible from the **ap:defaults:dualband** context of the CLI.

Syntax

```
led-mode off | normal
```

Parameters

off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.
normal	Identifies the AP status during the registration process during power on and boot process.

Examples

The following example turns off LED activity:

```
EWC.enterasys.com:ap:defaults:dualband# led-mode off
```

4.3.4.5 lldp

Use the **lldp** command to enable the broadcast of the LLDP protocol by a Wireless AP. Use the **no** form of the command to disable LLDP. The **lldp** command is accessible from the **ap:defaults:dualband** context of the CLI.

Syntax

```
lldp <Announcement Interval> <Announcement Delay>
no lldp
```

Parameters

<Announcement Interval>	Specifies the scheduled frequency, measured in seconds, in which the Wireless AP advertises its information by sending a new LLDP packet.
<Announcement Delay>	Specifies the delay, measured in seconds, between successive LLDP frame transmissions that is initiated by a value/status change in the LLDP local systems MIB.

Examples

The following example enables LLDP for the default Wireless AP configuration with an announcement interval of 30 seconds, and an announcement delay of 2.

```
EWC.enterasys.com:ap:defaults:dualband# lldp 30 2
```

If SNMP is enabled to publish on the Enterasys Wireless Controller and you enable LLDP, the following message is displayed:

```
WARNING: SNMP is set to publish. How Do you wish to continue?
(C) Cancel
(P) Proceed
(O) Disable SNMP publishing and proceed
```

Type one of the following:

- **C** – Cancels the LLDP configuration and returns to the AP context.
- **P** – Enables LLDP and maintains SNMP running
- **O** – Enables LLDP and disables SNMP publishing

4.3.4.6 persistent

Use the **persistent** command to enable mode persistence. Use the **no** form of the command to disable the feature. The **persistent** command is accessible from the **ap:defaults:dualband** context of the CLI.

Syntax

```
persistent
no persistent
```

Parameters

None

Examples

The following example enables mode persistence.

```
EWC.enterasys.com:ap:defaults:dualband# persistent
```

Note: After you have run the **persistent** command, you must run the **apply** command to implement the change in mode persistence value.

4.3.4.7 poll_timeout

Use the **poll_timeout** command to set the amount of time the Wireless AP will wait for a response time from the Enterasys Wireless Controller before rebooting. The **poll_timeout** command is accessible from the **ap:defaults:dualband** context of the CLI.

Syntax

```
poll_timeout <value>
```

Note: The acceptable range for poll_timeout value is from 3 to 600.

Parameters

<value>	Specifies the amount of time, in seconds, to wait for a response from the Enterasys Wireless Controller before rebooting.

Examples

The following example sets the poll timeout to 20 seconds

```
EWC.enterasys.com:ap:defaults:dualband# poll_timeout 20
```

Note: After you have run the **poll_timeout** command, you must run the **apply** command to implement the change in poll timeout value.

4.3.4.8 radio1

The **radio1** command refers to the **radio1** context, which contains commands to configure Radio 1 of the Wireless AP. The **radio1** command is accessible from the **ap:defaults:dualband** context of the CLI.

The following commands are available in the **ap:defaults:dualband:radio1** context:

- admin-mode
- atpc
- beaconp
- dcs — See dcs for commands in the **ap:defaults:dualband:radio1:dcs** context.
- divrx
- divtx
- domain
- dtim

- frag
- hwretries
- max-distance
- maxbrate
- maxoprate
- minbrate
- mode
- rts
- tx_adjust_power
- tx_max_power
- tx_min_power

4.3.4.8.1 admin-mode

Use this comment to configure the administration status for the radio. The **admin-mode** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
admin-mode off|on
```

Parameters

off	Clear the administrative status.
on	Set the administrative status. On is the default.

Examples

```
EWC.enterasys.com:ap:defaults:dualband:radio1# admin-mode on
```

4.3.4.8.2 atpc

Use the **atpc** command to enable Auto Tx Power Ctrl (ATPC). Use the **no** form of the command to disable the feature. The **atpc** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
atpc
no atpc [maintain_power]
```

Parameters

[maintain_power]	When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established.

Examples

The following example disables atpc on Radio 1.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# no atpc maintain_power
```

4.3.4.8.3 beaconp

Use the **beaconp** command to set time units between beacon transmissions. The **beaconp** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
beaconp <value>
```

Parameters

<value>	Specifies the number of time units (milliseconds) between beacon transmissions. The acceptable range for beaconp value is from 50 to 1000 milliseconds.

Examples

The following example sets the time between successive beacons to 70 ms on Radio 1.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# beaconp 70
```

4.3.4.8.4 dcs

The **dcs** command refers to the **dcs** context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The **dcs** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Note: Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

The following commands are available in the **ap:defaults:dualband:radio1:dcs** context:

- channel_plan
- mode
- noise_threshold
- occupancy_threshold
- radio_channels
- update_period

4.3.4.8.4.1 channel_plan

Use the **channel_plan** command to customize the channel plan for the Wireless AP's Radio 1. The **channel_plan** command is accessible from the **ap:defaults:dualband:radio1:dcs** context of the CLI.

Syntax

```
channel_plan <all-non-dfs|all|auto|3-channel|4-channel|channel
[, channel]>
```

Note: The parameters available in the **channel_plan** command are determined by the setting of the **mode** command in the **ap:defaults:dualband:radio1** context.

Parameters

all-non-dfs	Radio 1 uses all non-DFS channels.
all	Radio 1 uses all channels
auto	Radio 1 uses 3 channels for countries supporting 11 channels and 4 channels for countries supporting 13 channels.
3-channel	Radio 1 uses 3 channels.
4-channel	Radio 1 uses 4 channels.
channel[, channel]	Radio 1 uses the channels that are listed, separated by commas.

Examples

The following example shows the channel plan for radio 1 is configured to include all channels.

```
EWC:ap:defaults:dualband:radio1:dcs# channel_plan all-non-dfs
```

The following example shows that the channel plan for radio 1 is customized to include the following channels: 1, 2 and 3.

```
EWC.enterasys.com:ap:defaults:dualband:radio1:dcs# channel_plan 1, 2, 3
```

4.3.4.8.4.2 mode

Use the **mode** command to set the **DCS** mode. The **mode** command is accessible from the **ap:defaults:dualband:radio1:dcs** context of the CLI.

Syntax

```
mode <off|monitor|active>
```

Parameters

off	Disables DCS
monitor	Monitors the noise and interference on the current channel
active	Enables DCS

Note: In monitor mode, DCS generates an alarm and does not change the channel if the noise and interference levels on the current channel exceed beyond their thresholds. In active mode, DCS changes the channel if the noise and interference levels on the current channel exceed beyond their thresholds.

Examples

The following example sets DCS to active mode.

```
EWC.enterasys.com:ap:defaults:dualband:radio1:dcs# mode active
```

4.3.4.8.4.3 noise_threshold

Use the **noise_threshold** command to set the DCS noise threshold. The **noise_threshold** command is accessible from the **ap:defaults:dualband:radio1:dcs** context of the CLI.

Syntax

```
noise_threshold <thrshold>
```

Parameters

<thrshold>	Specifies the DCS noise threshold in dBm. The DCS noise threshold must be in the -95 to -50 range. ACS will scan for a new operating channel for the Wireless AP if the threshold is exceeded.

Examples

The following example sets the noise threshold to -45 dBm.

```
EWC.enterasys.com:ap:defaults:dualband:radio1:dcs# noise_threshold -45
```

4.3.4.8.4.4 occupancy_threshold

Use the **occupancy_threshold** command to set the DCS Channel Occupancy Threshold. The **occupancy_threshold** command is accessible from the **ap:defaults:dualband:radio1:dcs** context of the CLI.

Syntax

```
occupancy_threshold <thrshold>
```

Parameters

thrshold	Specifies the DCS Occupancy Threshold as a percentage. The DCS Occupancy Threshold must be in the 10 to 100 range.

Examples

The following example sets the DCS Channel Occupancy Threshold to 10 per cent.

```
EWC.enterasys.com:ap:defaults:dualband:radio1:dcs# occupancy_threshold 10
```

4.3.4.8.4.5 radio_channels

Use the **radio_channels** command to display the list of available radio channels for auto channel selection (ACS). The **radio_channels** command is accessible from the **ap:defaults:dualband:radio1:dcs** context of the CLI.

Syntax

```
radio_channels
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:defaults:dualband:radio1:dcs# radio_channels
Available radio channels:
        36: 5180 MHz
        40: 5200 MHz
        44: 5220 MHz
        48: 5240 MHz
        52: 5260 MHz
        56: 5280 MHz
        60: 5300 MHz
        64: 5320 MHz
        100: 5500 MHz
        104: 5520 MHz
        108: 5540 MHz
        112: 5560 MHz
        116: 5580 MHz
        120: 5600 MHz
        124: 5620 MHz
        128: 5640 MHz
        132: 5660 MHz
        136: 5680 MHz
        140: 5700 MHz
        149: 5745 MHz
        153: 5765 MHz
        157: 5785 MHz
        161: 5805 MHz
        165: 5825 MHz
```

4.3.4.8.4.6 update_period

Use the **update_period** command to set the DCS update period. — the time period during which the Wireless AP averages the DCS noise threshold and DCS channel occupancy threshold measurements. If either one of these thresholds is exceeded, the Wireless AP will trigger ACS. The **update_period** command is accessible from the **ap:defaults:dualband:radio1:dcs** context of the CLI.

Syntax

```
update_period <period>
```

Parameters

<period>	Specifies the time period, measured in minutes, during which the Wireless AP averages the DCS noise threshold and DCS channel occupancy threshold measurements. If either one of these thresholds is exceeded, then the Wireless AP will trigger ACS

Examples

The following example sets the DCS update period to 2 minutes.

```
EWC.enterasys.com:ap:defaults:dualband:radio1:dcs# update_period 2
```

4.3.4.8.5 divrx

Use the **divrx** command to select the best signal from the pair of diversity antennas for the reception of packets from client devices. Select **best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The **divrx** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
divrx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:dualband:radio1# divrx right
```

4.3.4.8.6 divtx

Use the **divtx** command to select the best signal from the pair of diversity antennas for the transmission of packets to client devices. Select **best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The **divtx** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
divtx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:dualband:radio1# divtx right
```

4.3.4.8.7 domain

Use the **domain** command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The **domain** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
domain <domain_name>
```

Note: The maximum length of the domain string is 15 characters.

Parameters

<domain_name>	Specifies the group name of APs that cooperate in managing RF channels.

Examples

The following example assigns the name **test** to the group of APs that cooperate in managing RF channels and transmission power levels.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# domain domain_test
```

4.3.4.8.8 dtim

Use the **dtim** command to set the Delivery Traffic Indication Message (DTIM) period. The **dtim** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
dtim <value>
```

Note: The acceptable range for the dtim value is from 1 to 255 beacon intervals.

Parameters

<value>	Specifies the DTIM period in beacons

Examples

The following example sets the Delivery Traffic Indication Message period to 2 beacons.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# dtim 2
```

4.3.4.8.9 frag

Use the **frag** command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold will be fragmented into packets that are less than or equal to this limit. The **frag** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
frag <value>
```

Parameters

<value>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery.

Examples

The following example sets the fragmentation threshold to 1500

```
EWC.enterasys.com:ap:defaults:dualband:radio1# frag 1500
```

4.3.4.8.10 hwretries

Use the **hwretries** command to set the number of retries for background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and turbo voice transmission queue. The **hwretries** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
hwretries (BK|BE|VI|VO|TVO) <value>
```

Parameters

BK	Specifies the number of retries for the Background transmission queue.
BE	Specifies the number of retries for the Best Effort transmission queue.
VI	Specifies the number of retries for the Video transmission queue.
VO	Specifies the number of retries for the Voice transmission queue.
TVO	Specifies the number of retries for the Turbo Voice transmission queue.

Examples

The following example sets the retry values for the background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and the turbo voice transmission queue as 1, 2, 3, 4, 5 respectively.

Note: You can set each parameter — background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue and turbo voice transmission queue — to any value from 0 to 10 (0 means adaptive).

```
EWC.enterasys.com:ap:defaults:dualband:radio1# hwretries 12345
```

4.3.4.8.11 max-distance

Use the **max-distance** command to set the maximum link distance, in meters, between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. If the link distance between APs is greater than the default value of 100 meters, configure the maximum distance up to 15,000 meters so that the software increases the timeout value proportionally with the distance between APs. The **max-distance** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Note: Do not change the default setting for any radio that is not participating in a Mesh or WDS.

Syntax

```
max-distance <value>
```

Parameters

<value>	Specifies the maximum distance between APs in meters. The default is 100 meters. You can enter a value from 100 to 15000 meters.

Examples

The following example sets the maximum distance between APs to 1500 meters.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# max-distance 1500
```

4.3.4.8.12 maxbrate

Use the **maxbrate** command to configure the maximum basic rate. The **maxbrate** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
maxbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps. The maximum basic rate choices adjust automatically to be higher or equal to the minimum basic rate.

Parameters

<value>	Specifies the maximum basic rate value in Mbps

Examples

The following example configures the maximum basic rate to 24 Mbps

```
EWC.enterasys.com:ap:defaults:dualband:radio1# maxbrate 24
```

4.3.4.8.13 maxoprate

Use the **maxoprate** command to set the maximum operational rate. The **maxoprate** is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Note: Available operational rate values (in Mbps) for Radio **1** are: 6, 9, 12, 18, 24, 36, 48, and 54.

Syntax

```
maxoprate <value>
```

Parameters

<value>	Specifies the maximum operational rate value in Mpbs

Examples

The following example sets the maximum operational rate to 24Mbps

```
EWC.enterasys.com:ap:defaults:dualband:radio1# maxoprate 24
```

4.3.4.8.14 minbrate

Use the **minbrate** command to configure the minimum basic rate. The **minbrate** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
minbrate <value>
```

Parameters

<value>	Specifies the minimum basic rate value in Mbps. The valid minbrate values are 6, 12 and 24 Mbps.

Examples

The following example configures the minimum basic rate to 6 Mbps

```
EWC.enterasys.com:ap:defaults:dualband:radio1# minbrate 6
```

4.3.4.8.15 mode

Use the **mode** command to set the radio options for Radio 1. Use the **no** form of the command to disable Radio 1. The **mode** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Syntax

```
mode <a|b|g|bg>
```

Note: Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Parameters

a	Enables 802.11a mode of Radio 1.
b	Enables the 802.11b-only mode of Radio 1. If enabled, the AP will use only 11b (CCK) rates with all associated clients
g	Enables the 802.11g-only mode of Radio 1. The AP will use 11g-only (OFDM) rates with all associated clients.
bg	Enables both the 802.11g mode and the 802.11b mode of Radio 1. If enabled, the AP will use 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients.

Examples

The following example enables only 802.11a mode of Radio 1.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# mode a
```

4.3.4.8.16 rts

Use the **rts** command to specify the size of the Request to Send (RTS) threshold. The **rts** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI

Syntax

```
rts <value>
```

Note: The acceptable value for rts value is from 1 to 2346.

Parameters

<value>	Specifies the Request to Send packet size threshold.

Examples

The following example sets the RTS packet size to 256

```
EWC.enterasys.com:ap:defaults:dualband:radio1# rts 256
```

4.3.4.8.17 tx_adjust_power

Use the **tx_adjust_power** command to specify an offset to the Tx power level, which is used to adjust the ATPC power levels from the calculated value. The **tx_adjust_power** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Note: The **tx_adjust_power** command is available only when Auto Tx Power Ctrl (ATPC) is enabled.

Syntax

```
tx_adjust_power <value>
```

Parameters

<value>	Specifies the value in dBm

Examples

The following example specifies the Tx power level to 0 dBm.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# tx_adjust_power 0
```

4.3.4.8.18 tx_max_power

Use the **tx_max_power** command to set the maximum Tx power level. The **tx_max_power** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Note: The **tx_max_power** is a maximum level when ATPC is enabled, and a fixed level when it ATPC is disabled.

Syntax

```
tx_max_power <value>
```

Parameters

<value>	Specifies the maximum Tx power level.

Examples

The following example sets the maximum Tx power level to 18 dBm.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# tx_max_power 18
```

4.3.4.8.19 tx_min_power

Use the **tx_min_power** command to specify the minimum Tx power level. The **tx_min_power** command is accessible from the **ap:defaults:dualband:radio1** context of the CLI.

Note: The tx_min_power is available only when Auto Tx Power Ctrl (ATPC) is enabled.

Syntax

```
tx_min_power <value>
```

Parameters

<value>	Specifies the value in dBm

Examples

The following example specifies the minimum Tx power level to 8 dBm.

```
EWC.enterasys.com:ap:defaults:dualband:radio1# tx_min_power 8
```

4.3.4.9 radio2

The **radio2** command refers to the **radio2** context, which contains commands to configure Radio 2 of the Wireless AP. The **radio2** command is accessible from the **ap:defaults:dualband** context of the CLI.

The following commands are available in the **ap:defaults:dualband:radio2** context:

- admin-mode
- atpc
- beaconp
- dcs — See dcs for commands in the **ap:defaults:dualband:radio2:dcs** context.
- divrx
- divtx
- domain
- dtim
- frag

- hwretries
- maxbrate
- maxoprate
- minbrate
- mode
- pmode
- prate
- preamble
- ptype
- rts
- tx_adjust_power
- tx_max_power
- tx_min_power

4.3.4.9.1 admin-mode

Use this comment to configure the administration status for the radio. The **admin-mode** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
admin-mode off|on
```

Parameters

off	Clear the administrative status.
on	Set the administrative status. On is the default.

Examples

```
EWC.enterasys.com:ap:defaults:dualband:radio2# admin-mode on
```

4.3.4.9.2 atpc

Use the **atpc** command to enable Auto Tx Power Ctrl (ATPC). Use the **no** form of the command to disable the feature. The **atpc** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
atpc
no atpc [maintain_power]
```

Parameters

[maintain_power]	When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established.

Examples

The following example disables atpc on Radio 2.

```
EWC.enterasys.com:ap:defaults:dualband:radio2# no atpc maintain_power
```

4.3.4.9.3 beaconp

Use the **beaconp** command to set time units between beacon transmissions. The **beaconp** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
beaconp <value>
```

Parameters

<value>	Specifies the number of time units (milliseconds) between beacon transmissions. The acceptable range for beaconp value is from 50 to 1000 milliseconds.

Examples

The following example sets the time between successive beacons to 70 ms on Radio 2.

```
EWC.enterasys.com:ap:defaults:dualband:radio2# beaconp 70
```

4.3.4.9.4 dcs

The **dcs** command refers to the **dcs** context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The **dcs** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Note: Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

The following commands are available in the **ap:defaults:dualband:radio2** context:

- channel_plan
- mode
- noise_threshold
- occupancy_threshold
- radio_channels
- update_period

4.3.4.9.4.1 channel_plan

Use the **channel_plan** command to customize the channel plan for the Wireless AP's Radio 2. The **channel_plan** command is accessible from the **ap:defaults:dualband:radio2:dcs** context of the CLI.

Syntax

```
channel_plan <all-non-dfs|all|auto|3-channel|4-channel|channel
[, channel]>
```

Note: The parameters available in the **channel_plan** command are determined by the setting of the **mode** command in the **ap:defaults:dualband:radio2** context.

Parameters

all-non-dfs	Radio 2 uses all non-DFS channels.
all	Radio 2 uses all channels
auto	Radio 2 uses 3 channels for countries supporting 11 channels and 4 channels for countries supporting 13 channels.
3-channel	Radio 2 uses 3 channels.
4-channel	Radio 2 uses 4 channels.
channel[, channel]	Radio 2 uses the channels that are listed, separated by commas.

Examples

The following example indicates that the channel plan for radio 2 is customized to include all non-DFS channels.

```
EWC.enterasys.com:ap:defaults:dualband:radio2:dcs# channel_plan all-non-dfs
```

The following example shows that the channel plan for radio 2 is customized to include the following channels: 1, 2 and 3.

```
EWC.enterasys.com:ap:defaults:dualband:radio2:dcs# channel_plan 1, 2, 3
```

4.3.4.9.4.2 mode

Use the **mode** command to set the **DCS** mode. The **mode** command is accessible from the **ap:defaults:dualband:radio2:dcs** context of the CLI.

Syntax

```
mode <off|monitor|active>
```

Parameters

off	Disables DCS
monitor	Monitors the noise and interference on the current channel
active	Enables DCS

Note: In monitor mode, DCS generates an alarm and does not change the channel if the noise and interference levels on the current channel exceed beyond their thresholds. In active mode, DCS changes the channel if the noise and interference levels on the current channel exceed beyond their thresholds.

Examples

The following example sets DCS to active mode.

```
EWC.enterasys.com:ap:defaults:dualband:radio2:dcs# mode active
```

4.3.4.9.4.3 noise_threshold

Use the **noise_threshold** command to set the DCS noise threshold. The **noise_threshold** command is accessible from the **ap:defaults:dualband:radio2:dcs** context of the CLI.

Syntax

```
noise_threshold <thrshold>
```

Parameters

<thrshold>	Specifies the DCS noise threshold in dBm. The DCS noise threshold must be in the -95 to -50 range. ACS will scan for a new operating channel for the Wireless AP if the threshold is exceeded.

Examples

The following example sets the noise threshold to -45 dBm.

```
EWC.enterasys.com:ap:defaults:dualband:radio2:dcs# noise_threshold -45
```

4.3.4.9.4.4 occupancy_threshold

Use the **occupancy_threshold** command to set the DCS Channel Occupancy Threshold. The **occupancy_threshold** command is accessible from the **ap:defaults:dualband:radio2:dcs** context of the CLI.

Syntax

```
occupancy_threshold <thrshold>
```

Parameters

thrshold	Specifies the DCS Occupancy Threshold as a percentage. The DCS Occupancy Threshold must be in the 10 to 100 range.

Examples

The following example sets the DCS Channel Occupancy Threshold to 10 per cent.

```
EWC.enterasys.com:ap:defaults:dualband:radio2:dcs# occupancy_threshold 10
```

4.3.4.9.4.5 radio_channels

Use the **radio_channels** command to display the list of available radio channels for auto channel selection (ACS). The **radio_channels** command is accessible from the **ap:defaults:dualband:radio2:dcs** context of the CLI.

Syntax

```
radio_channels
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:defaults:dualband:radio2:dcs# radio_channels
Available radio channels:
        1: 2412 MHz
        2: 2417 MHz
        3: 2422 MHz
        4: 2427 MHz
        5: 2432 MHz
        6: 2437 MHz
        7: 2442 MHz
        8: 2447 MHz
        9: 2452 MHz
        10: 2457 MHz
        11: 2462 MHz
```

4.3.4.9.4.6 update_period

Use the **update_period** command to set the DCS update period — the time period during which the Wireless AP averages the DCS noise threshold and DCS channel occupancy threshold measurements. If either one of these thresholds is exceeded, the Wireless AP will trigger ACS. The **update_period** command is accessible from the **ap:defaults:dualband:radio2:dcs** context of the CLI.

Syntax

```
update_period <period>
```

Parameters

<period>	Specifies the time period, measured in minutes, during which the Wireless AP averages the DCS noise threshold and DCS channel occupancy threshold measurements. If either one of these thresholds is exceeded, then the Wireless AP will trigger ACS

Examples

The following example sets the DCS update period to 2 minutes.

```
EWC.enterasys.com:ap:defaults:dualband:radio2:dcs# update_period 2
```

4.3.4.9.5 divrx

Use the **divrx** command to select the best signal from the pair of diversity antennas for the reception of packets from client devices. Select **best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The **divrx** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
divrx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:dualband:radio2# divrx right
```

4.3.4.9.6 divtx

Use the **divtx** command to select the best signal from the pair of diversity antennas for the transmission of packets to client devices. Select **best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The **divtx** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
divtx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:dualband:radio2# divtx right
```

4.3.4.9.7 domain

Use the **domain** command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The **domain** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
domain <domain_name>
```

Note: The maximum length of the domain string is 15 characters.

Parameters

<domain_name>	Specifies the group name of APs that cooperate in managing RF channels.

Examples

The following example assigns the name **test** to the group of APs that cooperate in managing RF channels and transmission power levels.

```
EWC.enterasys.com:ap:defaults:dualband:radio2# domain test
```

4.3.4.9.8 dtim

Use the **dtim** command to set the Delivery Traffic Indication Message (DTIM) period. The **dtim** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
dtim <value>
```

Note: The acceptable range for the dtim value is from 1 to 255 beacon intervals.

Parameters

<value>	Specifies the DTIM period in beacons

Examples

The following example sets the Delivery Traffic Indication Message period to 2 beacons.

```
EWC.enterasys.com:ap:defaults:dualband:radio2# dtim 2
```

4.3.4.9.9 frag

Use the **frag** command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold will be fragmented into packets that are less than or equal to this limit. The **frag** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
frag <value>
```

Parameters

<value>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery.

Examples

The following example sets the fragmentation threshold to 1500

```
EWC.enterasys.com:ap:defaults:dualband:radio2# frag 1500
```

4.3.4.9.10 hwretries

Use the **hwretries** command to set the number of retries for background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and turbo voice transmission queue. The **hwretries** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
hwretries (BK|BE|VI|VO|TVO) <value>
```

Parameters

BK	Specifies the number of retries for the Background transmission queue.
BE	Specifies the number of retries for the Best Effort transmission queue.
VI	Specifies the number of retries for the Video transmission queue.
VO	Specifies the number of retries for the Voice transmission queue.
TVO	Specifies the number of retries for the Turbo Voice transmission queue.

Examples

The following example sets the retry values for the background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and the turbo voice transmission queue as 1, 2, 3, 4, 5 respectively.

Note: You can set each parameter — background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue and turbo voice transmission queue — to any value from 0 to 10 (0 means adaptive).

```
EWC.enterasys.com:ap:defaults:dualband:radio2# hwretries 12345
```

4.3.4.9.11 maxbrate

Use the **maxbrate** command to configure the maximum basic rate. The **maxbrate** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
maxbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps. The maximum basic rate choices adjust automatically to be higher or equal to the minimum basic rate.

Parameters

<value>	Specifies the maximum basic rate value in Mbps

Examples

The following example configures the maximum basic rate to 24 Mbps

```
EWC.enterasys.com:ap:defaults:dualband:radio2# maxbrate 24
```

4.3.4.9.12 maxoprate

Use the **maxoprate** command to set the maximum operational rate. The **maxoprate** is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Note: Available operational rate values (in Mbps) for Radio 2 are: 6, 9, 12, 18, 24, 36, 48, and 54.

Syntax

```
maxoprate <value>
```

Parameters

<value>	Specifies the maximum operational rate value in Mpbs

Examples

The following example sets the maximum operational rate to 24Mbps

```
EWC.enterasys.com:ap:defaults:dualband:radio2# maxoprate 24
```

4.3.4.9.13 minbrate

Use the **minbrate** command to configure the minimum basic rate. The **minbrate** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
minbrate <value>
```

Parameters

<value>	Specifies the minimum basic rate value in Mbps. The valid minbrate values are 6, 12 and 24 Mbps.

Examples

The following example configures the minimum basic rate to 6 Mbps

```
EWC.enterasys.com:ap:defaults:dualband:radio2# minbrate 6
```

4.3.4.9.14 mode

Use the **mode** command to set the radio options for Radio 2. Use the **no** form of the command to disable Radio 2. The **mode** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
mode <a|b|g|bg>
```

Note: Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Parameters

a	Enables the 802.11a-only mode of Radio 2.
b	Enables the 802.11b-only mode of Radio 2. If enabled, the AP will use only 11b (CCK) rates with all associated clients.
g	Enables the 802.11g-only mode of Radio 2. The AP will use 11g-only (OFDM) rates with all associated clients.
bg	Enables both the 802.11g mode and the 802.11b mode of Radio 2. If enabled, the AP will use 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients.

Examples

The following example enables only 802.11b mode of Radio 2.

```
EWC.enterasys.com:ap:defaults:dualband:radio2# mode b
```

4.3.4.9.15 pmode

Use the **pmode** command to configure the Protection Mode, which will protect 802.11g client transmissions from interruption by 802.11b clients. The **pmode** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
pmode (none|auto|always)
```

Parameters

none	Deactivates Protection Mode
auto	Indicates that Protection Mode will be used only when 802.11b clients or Wireless APs are detected
always	Indicates that Protection Mode will remain active at all times

Caution: Only use **none** if the Wireless AP will NOT be servicing 802.11b clients, and there are no 802.11b clients or Wireless APs sharing the same air space.

Examples

The following example configures the Wireless AP to use Protection Mode at all times

```
EWC.enterasys.com:ap:defaults:dualband:radio2# pmode always
```

4.3.4.9.16 prate

Use the **prate** command to adjust the Protection Rate. The **prate** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
prate (1|2|5.5|11)
```

Parameters

1|2|5.5|11	Specifies the Protection Rate in Mbps

Examples

The following example adjusts the Protection Rate to 5.5 Mbps

```
EWC.enterasys.com:ap:defaults:dualband:radio2# prate 5.5
```

4.3.4.9.17 preamble

Use the **preamble** command to set the preamble type. The **preamble** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
preamble (short|long|auto)
```

Parameters

short	Specifies short preambles
long	Specifies long preambles
auto	Indicates that preamble types will be automatically selected by the Wireless AP

Note: For preambles set to auto, the Wireless AP will use short preambles, unless clients using the original 802.11 standard are detected.

Examples

The following example enables the long option for the preamble type

```
EWC.enterasys.com:ap:defaults:dualband:radio2# preamble long
```

4.3.4.9.18 ptype

Use the **ptype** command to select the Protection Type. The **ptype** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Syntax

```
ptype (cts only|rts cts)
```

Parameters

cts only	Specifies the Clear to Send (CTS) type
rts cts	Specifies the Request to Send (RTS) and Clear to Send (CTS) types

Examples

The following example sets the protection type to CTS

```
EWC.enterasys.com:ap:defaults:dualband:radio2# ptype cts only
```

4.3.4.9.19 rts

Use the **rts** command to specify the size of the Request to Send (RTS) threshold. The **rts** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI

Syntax

```
rts <value>
```

Note: The acceptable value for rts value is from 1 to 2346.

Parameters

<value>	Specifies the Request to Send packet size threshold.

Examples

The following example sets the RTS packet size to 256

```
EWC.enterasys.com:ap:defaults:dualband:radio2# rts 256
```

4.3.4.9.20 tx_adjust_power

Use the **tx_adjust_power** command to specify an offset to the Tx power level, which is used to adjust the ATPC power levels from the calculated value. The **tx_adjust_power** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Note: The **tx_adjust_power** command is available only when Auto Tx Power Ctrl (ATPC) is enabled.

Syntax

```
tx_adjust_power <value>
```

Parameters

<value>	Specifies the value in dBm

Examples

The following example specifies the Tx power level to 0 dBm.

```
EWC.enterasys.com:ap:defaults:dualband:radio2# tx_adjust_power 0
```

4.3.4.9.21 tx_max_power

Use the **tx_max_power** command to set the maximum Tx power level. The **tx_max_power** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Note: The **tx_max_power** is a maximum level when ATPC is enabled, and a fixed level when it ATPC is disabled.

Syntax

```
tx_max_power <value>
```

Parameters

<value>	Specifies the maximum Tx power level.

Examples

The following example sets the maximum Tx power level to 18 dBm.

```
EWC.enterasys.com:ap:defaults:dualband:radio2# tx_max_power 18
```

4.3.4.9.22 tx_min_power

Use the **tx_min_power** command to specify the minimum Tx power level. The **tx_min_power** command is accessible from the **ap:defaults:dualband:radio2** context of the CLI.

Note: The **tx_min_power** is available only when Auto Tx Power Ctrl (ATPC) is enabled.

Syntax

```
tx_min_power <value>
```

Parameters

<value>	Specifies the value in dBm

Examples

The following example specifies the minimum Tx power level to 8 dBm.

```
EWC.enterasys.com:ap:defaults:dualband:radio2# tx_min_power 8
```

4.3.4.10 telnet

Use the **telnet** command to enable telnet access to the Wireless AP. Use the **no** form of the command to disable it. The **telnet** command is accessible from the **ap:defaults:dualband** context of the CLI.

Syntax

```
telnet
no telnet
```

Parameters

None

Examples

The following example enables telnet access to the Wireless AP

```
EWC.enterasys.com:ap:defaults:dualband# telnet
```

Note: After you have run the **telnet** command, you must run the **apply** command to implement the change.

4.3.5 learnac

Use the **learnac** command to allow the Wireless AP to provide its own EWC Search List. Use **no** form of the command to disable this feature. The **learnac** command is accessible from the **ap:defaults** context of the CLI.

Note: If you disallow the Wireless AP to provide its own EWC Search List, you should specify the controller's static IP address by running the **aclist** command. For more information, see "aclist" on page 4-146.
If you disallow the Wireless AP to provide its own EWC Search List and do not specify the controller's static IP address, the Wireless AP will use the SLP to discover the controller.

Syntax

```
learnac
no learnac
```

Parameters

None

Examples

The following example allows each Wireless AP to provide its own **EWC Search List**.

```
EWC.enterasys.com:ap:defaults# learnac
```

Note: After you have run the **learnac** command, you must run the **apply** command to implement the changes.

4.3.6 std

The **std** command refers to context **std**, which contains commands to configure the default AP settings for the standard Wireless AP. The **std** command is accessible from the **ap:defaults** context of the CLI.

The following commands are available in the **ap:defaults:std** context:

- bcast_disassoc
- client_session
- country
- led-mode
- lldp
- poll_timeout
- radio1 — See radio1 for commands in the **ap:defaults:std:radio1** context.
- radio2 — See radio2 for commands in the **ap:defaults:std:radio2** context.
- telnet

4.3.6.1 bcast_disassoc

Use the **bcast_disassoc** command to enable the Wireless AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. Use the **no** form of the

command to disable the feature. The **bcast_disassoc** command is accessible from the **ap:defaults:std** context of the CLI.

Syntax

```
bcast_disassoc
no bcast_disassoc
```

Parameters

None

Examples

The following disassociates clients from the Wireless AP

```
EWC.enterasys.com:ap:defaults:std# bcast_disassoc
```

Note: After you have run the **bcast_disassoc** command, you must run the **apply** command to implement the change in broadcast disassociation.

4.3.6.2 client_session

Use the **client_session** command to enable users to maintain client sessions in the event of a poll failure. Use the **no** form of the command to disable the feature. The **client_session** command is accessible from the **ap:defaults:std** context of the CLI.

Syntax

```
client_session
no client_session
```

Parameters

None

Examples

The following example enables user client sessions

```
EWC.enterasys.com:ap:defaults:std# client_session
```

Note: After you have run the **client_session** command, you must run the **apply** command to implement the change in client session.

4.3.6.3 country

Use the **country** command to specify the country the Wireless AP resides in. The **country** command is accessible from the **ap:defaults:std** context of the CLI.

Syntax

```
country <country_name>
```

Parameters

<country_name>	Specifies the name of the country

Examples

The following example sets the name of the country to United States.

```
EWC.enterasys.com:ap:defaults:std# country United States
```

Note: After you have run the **country** command, you must run the **apply** command to implement the change in country.

4.3.6.4 led-mode

Use the **led-mode** command to configure the behavior of the LEDs on the Wireless AP. The **led-mode** command is accessible from the **ap:defaults:std** context of the CLI.

Syntax

```
led-mode off | normal
```

Parameters

off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.
normal	Identifies the AP status during the registration process during power on and boot process.

Examples

The following example turns off LED activity:

```
EWC.enterasys.com:ap:defaults:std# led-mode off
```

4.3.6.5 lldp

Use the **lldp** command to enable the broadcast of the LLDP protocol by a Wireless AP. Use the **no** form of the command to disable LLDP. The **lldp** command is accessible from the **ap:defaults:std** context of the CLI.

Syntax

```
lldp <Announcement Interval> <Announcement Delay>
no lldp
```

Parameters

<Announcement Interval>	Specifies the scheduled frequency, measured in seconds, in which the Wireless AP advertises its information by sending a new LLDP packet.
<Announcement Delay>	Specifies the delay, measured in seconds, between successive LLDP frame transmissions that is initiated by a value/status change in the LLDP local systems MIB.

Examples

The following example enables LLDP for the default Wireless AP configuration with an announcement interval of 30 seconds, and an announcement delay of 2.

```
EWC.enterasys.com:ap:defaults:std# lldp 30 2
```

If SNMP is enabled to publish on the Enterasys Wireless Controller and you enable LLDP, the following message is displayed:

```
WARNING: SNMP is set to publish. How Do you wish to continue?
(C) Cancel
(P) Proceed
(O) Disable SNMP publishing and proceed
```

Type one of the following:

- **C** – Cancels the LLDP configuration and returns to the AP context.
- **P** – Enables LLDP and maintains SNMP running
- **O** – Enables LLDP and disables SNMP publishing

4.3.6.6 persistent

Use the **persistent** command to enable mode persistence. Use the **no** form of the command to disable the feature. The **persistent** command is accessible from the **ap:defaults:std** context of the CLI.

Syntax

```
persistent
no persistent
```

Parameters

None

Examples

The following example enables mode persistence.

```
EWC.enterasys.com:ap:defaults:std# persistent
```

Note: After you have run the **persistent** command, you must run the **apply** command to implement the change in mode persistence value.

4.3.6.7 poll_timeout

Use the **poll_timeout** command to set the amount of time the Wireless AP will wait for a response time from the Enterasys Wireless Controller before rebooting. The **poll_timeout** command is accessible from the **ap:defaults:std** context of the CLI.

Syntax

```
poll_timeout <value>
```

Note: The acceptable range for poll_timeout value is from 3 to 600.

Parameters

<value>	Specifies the amount of time, in seconds, to wait for a response from the Enterasys Wireless Controller before rebooting.

Examples

The following example sets the poll timeout to 20 seconds

```
EWC.enterasys.com:ap:defaults:std# poll_timeout 20
```

Note: After you have run the **poll_timeout** command, you must run the **apply** command to implement the change in poll timeout value.

4.3.6.8 radio1

The **radio1** command refers to the **radio1** context, which contains commands to configure Radio 1 of the Wireless AP. The **radio1** command is accessible from the **ap:defaults:std** context of the CLI.

The following commands are available in the **ap:defaults:std:radio1** context:

- admin-mode
- atpc
- beaconp
- dcs — See dcs for commands in the **ap:defaults:std:radio1:dcs** context.
- divrx
- divtx
- domain
- dtim
- frag
- hwretries
- maxbrate
- maxoprate
- max-distance
- minbrate
- mode
- rts
- tx_max_power

4.3.6.8.1 admin-mode

Use this comment to configure the administration status for the radio. The **admin-mode** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
admin-mode off|on
```

Parameters

off	Clear the administrative status.
on	Set the administrative status. On is the default.

Examples

```
EWC.enterasys.com:ap:defaults:std:radio1# admin-mode on
```

4.3.6.8.2 atpc

Use the **atpc** command to enable Auto Tx Power Ctrl (ATPC). Use the **no** form of the command to disable the feature. The **atpc** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
atpc
no atpc
```

Parameters

None

Examples

The following example disables ATPC on Radio 1.

```
EWC.enterasys.com:ap:defaults:std:radio1# no atpc
```

4.3.6.8.3 beaconp

Use the **beaconp** command to set time units between beacon transmissions. The **beaconp** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
beaconp <value>
```

Parameters

<value>	Specifies the number of time units (milliseconds) between beacon transmissions. The acceptable range for beaconp value is from 50 to 1000 milliseconds.

Examples

The following example sets the time between successive beacons to 70 ms on Radio 1.

```
EWC.enterasys.com:ap:defaults:std:radio1# beaconp 70
```

4.3.6.8.4 dcs

The **dcs** command refers to the **dcs** context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The **dcs** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Note: Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

The following commands are available in the **ap:defaults:std:radio1:dcs** context:

- channel_plan
- mode
- radio_channels

4.3.6.8.4.1 channel_plan

Use the **channel_plan** command to customize the channel plan for the Wireless AP's Radio 1. The **channel_plan** command is accessible from the **ap:defaults:std:radio1:dcs** context of the CLI.

Syntax

```
channel_plan <all-non-dfs|all|channel[, channel]>
```

Note: The parameters available in the **channel_plan** command are determined by the setting of the **mode** command in the **ap:defaults:std:radio1** context.

Parameters

all-non-dfs	Radio 1 uses all non-DFS channels.
all	Radio 1 uses all channels
channel[, channel]	Radio 1 uses the channels that are listed, separated by commas.

Examples

The following example shows the channel plan for Radio 1 is configured to include all non-DFS channels.

```
EWC.enterasys.com:ap:defaults:std:radio1:dcs# channel_plan all-non-dfs
```

The following example shows the channel plan for Radio 1 is configured to include channels 1, 2, and 3.

```
EWC.enterasys.com:ap:defaults:std:radio1:dcs# channel_plan 1, 2, 3
```

4.3.6.8.4.2 mode

Use the **mode** command to set the **DCS** mode. The **mode** command is accessible from the **ap:defaults:std:radio1:dcs** context of the CLI.

Syntax

```
mode <off|monitor|active>
```

Parameters

off	Disables DCS
monitor	Monitors the noise and interference on the current channel
active	Enables DCS

Note: In monitor mode, DCS generates an alarm and does not change the channel if the noise and interference levels on the current channel exceed beyond their thresholds. In active mode, DCS changes the channel if the noise and interference levels on the current channel exceed beyond their thresholds.

Examples

The following example sets DCS to active mode.

```
EWC.enterasys.com:ap:defaults:std:radio1:dcs# mode active
```

4.3.6.8.4.3 radio_channels

Use the **radio_channels** command to display the list of available radio channels for auto channel selection (ACS). The **radio_channels** command is accessible from the **ap:defaults:std:radio1:dcs** context of the CLI.

Syntax

```
radio_channels
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:defaults:std:radio1:dcs# radio_channels
Available radio channels:
        36: 5180 MHz
        40: 5200 MHz
        44: 5220 MHz
        48: 5240 MHz
        52: 5260 MHz
        56: 5280 MHz
        60: 5300 MHz
        64: 5320 MHz
        100: 5500 MHz
        104: 5520 MHz
        108: 5540 MHz
        112: 5560 MHz
        116: 5580 MHz
        120: 5600 MHz
        124: 5620 MHz
        128: 5640 MHz
        132: 5660 MHz
```

```
136: 5680 MHz
140: 5700 MHz
149: 5745 MHz
153: 5765 MHz
157: 5785 MHz
161: 5805 MHz
165: 5825 MHz
```

4.3.6.8.5 divrx

Use the **divrx** command to select the best signal from the pair of diversity antennas for the reception of packets from client devices. Select **best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The **divrx** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
divrx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:std:radio1# divrx right
```

4.3.6.8.6 divtx

Use the **divtx** command to select the best signal from the pair of diversity antennas for the transmission of packets to client devices. Select **best** for the best signal from both antennas, or **left** or **right** to choose either of the two diversity antennas. The **divtx** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
divtx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:std:radio1# divtx right
```

4.3.6.8.7 domain

Use the **domain** command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The **domain** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
domain <domain_name>
```

Note: The maximum length of the domain string is 15 characters.

Parameters

<domain_name>	Specifies the group name of APs that cooperate in managing RF channels.

Examples

The following example assigns the name **test** to the group of APs that cooperate in managing RF channels and transmission power levels.

```
EWC.enterasys.com:ap:defaults:std:radio1# domain domain_test
```

4.3.6.8.8 dtim

Use the **dtim** command to set the Delivery Traffic Indication Message (DTIM) period. The **dtim** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
dtim <value>
```

Note: The acceptable range for the dtim value is from 1 to 255 beacon intervals.

Parameters

<value>	Specifies the DTIM period in beacons

Examples

The following example sets the Delivery Traffic Indication Message period to 2 beacons.

```
EWC.enterasys.com:ap:defaults:std:radio1# dtim 2
```

4.3.6.8.9 frag

Use the **frag** command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold will be fragmented into packets

that are less than or equal to this limit. The **frag** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
frag <value>
```

Parameters

<value>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery.

Examples

The following example sets the fragmentation threshold to 1500

```
EWC.enterasys.com:ap:defaults:std:radio1# frag 1500
```

4.3.6.8.10 hwretries

Use the **hwretries** command to set the number of retries for background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and turbo voice transmission queue. The **hwretries** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
hwretries (BK|BE|VI|VO|TVO) <value>
```

Parameters

BK	Specifies the number of retries for the Background transmission queue.
BE	Specifies the number of retries for the Best Effort transmission queue.
VI	Specifies the number of retries for the Video transmission queue.
VO	Specifies the number of retries for the Voice transmission queue.
TVO	Specifies the number of retries for the Turbo Voice transmission queue.

Examples

The following example sets the retry values for the background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and the turbo voice transmission queue as 1, 2, 3, 4, 5 respectively.

Note: You can set each parameter — background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue and turbo voice transmission queue — to any value from 0 to 10 (0 means adaptive).

```
EWC.enterasys.com:ap:defaults:std:radio1# hwretries 12345
```

4.3.6.8.11 maxbrate

Use the **maxbrate** command to configure the maximum basic rate. The **maxbrate** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
maxbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps. The maximum basic rate choices adjust automatically to be higher or equal to the minimum basic rate.

Parameters

<value>	Specifies the maximum basic rate value in Mbps

Examples

The following example configures the maximum basic rate to 24 Mbps

```
EWC.enterasys.com:ap:defaults:std:radio1# maxbrate 24
```

4.3.6.8.12 maxoprate

Use the **maxoprate** command to set the maximum operational rate. The **maxoprate** is accessible from the **ap:defaults:std:radio1** context of the CLI.

Note: Available operational rate values (in Mbps) for Radio **1** are: 6, 9, 12, 18, 24, 36, 48, and 54.

Syntax

```
maxoprate <value>
```

Parameters

<value>	Specifies the maximum operational rate value in Mpbs

Examples

The following example sets the maximum operational rate to 24Mbps

```
EWC.enterasys.com:ap:defaults:std:radio1# maxoprate 24
```

4.3.6.8.13 max-distance

Use the **max-distance** command to set the maximum link distance, in meters, between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. If the link distance between APs is greater than the default value of 100 meters, configure the maximum distance up to 15,000 meters so that the software increases the timeout value proportionally with the distance

between APs. The **max-distance** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Note: Do not change the default setting for any radio that is not participating in a Mesh or WDS.

Syntax

```
max-distance <value>
```

Parameters

<value>	Specifies the maximum distance between APs in meters. The default is 100 meters. You can enter a value from 100 to 15000 meters.

Examples

The following example sets the maximum distance between APs to 1500 meters.

```
EWC.enterasys.com:ap:defaults:std:radio1# max-distance 1500
```

4.3.6.8.14 minbrate

Use the **minbrate** command to configure the minimum basic rate. The **minbrate** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
minbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps.

Parameters

<value>	Specifies the minimum basic rate value in Mbps

Examples

The following example configures the minimum basic rate to 6 Mbps

```
EWC.enterasys.com:ap:defaults:std:radio1# minbrate 6
```

4.3.6.8.15 mode

Use the **mode** command to set the radio options for Radio 1. Use the **no** form of the command to disable Radio 1. The **mode** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Syntax

```
mode <a>
```

Note: Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Parameters

a	Enable 802.11a mode of Radio 1.

Examples

The following example enables only 802.11a mode of Radio 1.

```
EWC.enterasys.com:ap:defaults:std:radio1# mode a
```

4.3.6.8.16 rts

Use the **rts** command to specify the size of the Request to Send (RTS) threshold. The **rts** command is accessible from the **ap:defaults:std:radio1** context of the CLI

Syntax

```
rts <value>
```

Note: The acceptable value for rts value is from 1 to 2346.

Parameters

<value>	Specifies the Request to Send packet size threshold.

Examples

The following example sets the RTS packet size to 256

```
EWC.enterasys.com:ap:defaults:std:radio1# rts 256
```

4.3.6.8.17 tx_max_power

Use the **tx_max_power** command to set the maximum Tx power level. The **tx_max_power** command is accessible from the **ap:defaults:std:radio1** context of the CLI.

Note: The **tx_max_power** is a maximum level when ATPC is enabled, and a fixed level when it ATPC is disabled.

Syntax

```
tx_max_power <value>
```

Parameters

<value>	Specifies the maximum Tx power level.

Examples

The following example sets the maximum Tx power level to 18 dBm.

```
EWC.enterasys.com:ap:defaults:std:radio1# tx_max_power 18
```

4.3.6.9 radio2

The **radio2** command refers to the **radio2** context, which contains commands to configure Radio 2 of the Wireless AP. The **radio2** command is accessible from the **ap:defaults:std** context of the CLI.

The following commands are available in the **ap:defaults:std:radio2** context:

- admin-mode
- atpc
- beaconp
- dcs— See dcs for commands in the **ap:defaults:std:radio2:dcs** context
- divrx
- divtx
- domain
- dtim
- frag
- hwretries
- maxbrate
- max-distance
- maxoprate
- minbrate
- mode
- pmode
- prate
- preamble
- ptype
- rts
- tx_max_power

4.3.6.9.1 admin-mode

Use this comment to configure the administration status for the radio. The **admin-mode** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
admin-mode off|on
```

Parameters

off	Clear the administrative status.
on	Set the administrative status. On is the default.

Examples

```
EWC.enterasys.com:ap:defaults:std:radio2# admin-mode on
```

4.3.6.9.2 atpc

Use the **atpc** command to enable Auto Tx Power Ctrl (ATPC). Use the **no** form of the command to disable the feature. The **atpc** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
atpc
no atpc [maintain_power]
```

Parameters

[maintain_power]	When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established.

Examples

The following example disables atpc on Radio 2.

```
EWC.enterasys.com:ap:defaults:std:radio2# no atpc maintain_power
```

4.3.6.9.3 beaconp

Use the **beaconp** command to set time units between beacon transmissions. The **beaconp** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
beaconp <value>
```

Parameters

<value>	Specifies the number of time units (milliseconds) between beacon transmissions. The acceptable range for beaconp value is from 50 to 1000 milliseconds.

Examples

The following example sets the time between successive beacons to 70 ms on Radio 2.

```
EWC.enterasys.com:ap:defaults:std:radio2# beaconp 70
```

4.3.6.9.4 dcs

The **dcs** command refers to the **dcs** context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The **dcs** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Note: Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

The following commands are available in the **ap:defaults:std:radio2:dcs** context:

- channel_plan
- mode

- radio_channels

4.3.6.9.4.1 channel_plan

Use the **channel_plan** command to customize the channel plan for the Wireless AP's radio. The **channel_plan** command is accessible from the **ap:defaults:std:radio2:dcs** context of the CLI.

Syntax

```
channel_plan <auto|3-channel|4-channel|channel[, channel]>
```

Note: The parameters available in the **channel_plan** command are determined by the setting of the **mode** command in the **ap:defaults:std:radio2** context.

Parameters

auto	Radio 2 uses 3 channels for countries supporting 11 channels and 4 channels for countries supporting 13 channels
3-channel	Radio 2 uses 3 channels
4-channel	Radio 2 uses 4 channels
channel[, channel]	Radio 2 uses the channels that are listed, separated by commas

Example

The following example shows that the channel plan for radio 2 is customized to include the following channels: 1, 2 and 3.

```
EWC.enterasys.com:ap:defaults:std:radio2:dcs# channel_plan 1, 2, 3
```

4.3.6.9.4.2 mode

Use the **mode** command to set the **DCS** mode. The **mode** command is accessible from the **ap:defaults:std:radio2:dcs** context of the CLI.

Syntax

```
mode <off|monitor|active>
```

Parameters

off	Disables DCS
monitor	Monitors the noise and interference on the current channel
active	Enables DCS

Note: In monitor mode, DCS generates an alarm and does not change the channel if the noise and interference levels on the current channel exceed beyond their thresholds. In active mode, DCS changes the channel if the noise and interference levels on the current channel exceed beyond their thresholds.

Examples

The following example sets DCS to active mode.

```
EWC.enterasys.com:ap:defaults:std:radio2:dcs# mode active
```

4.3.6.9.4.3 radio_channels

Use the **radio_channels** command to display the list of available radio channels for auto channel selection (ACS). The **radio_channels** command is accessible from the **ap:defaults:std:radio2:dcs** context of the CLI.

Syntax

```
radio_channels
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:defaults:std:radio2:dcs# radio_channels
Available radio channels:
        1: 2412 MHz
        2: 2417 MHz
        3: 2422 MHz
        4: 2427 MHz
        5: 2432 MHz
        6: 2437 MHz
        7: 2442 MHz
        8: 2447 MHz
        9: 2452 MHz
        10: 2457 MHz
        11: 2462 MHz
```

4.3.6.9.5 divrx

Use the **divrx** command to select the best signal from the pair of diversity antennas for the reception of packets from client devices. Select **best** for the best signal from both antennas, or **left** or **right** to choose either of the two diversity antennas. The **divrx** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
divrx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:std:radio2# divrx right
```

4.3.6.9.6 divtx

Use the **divtx** command to select the best signal from the pair of diversity antennas for the transmission of packets to client devices. Select **best** for the best signal from both antennas, or **Left**

or **Right** to choose either of the two diversity antennas. The **divtx** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
divtx (best|left|right)
```

Parameters

best | left | right	Specifies the antenna for selection

Examples

The following example selects the right antenna

```
EWC.enterasys.com:ap:defaults:std:radio2# divtx right
```

4.3.6.9.7 domain

Use the **domain** command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The **domain** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
domain <domain_name>
```

Note: The maximum length of the domain string is 15 characters.

Parameters

<domain_name>	Specifies the group name of APs that cooperate in managing RF channels.

Examples

The following example assigns the name **test** to the group of APs that cooperate in managing RF channels and transmission power levels.

```
EWC.enterasys.com:ap:defaults:std:radio2# domain test
```

4.3.6.9.8 dtim

Use the **dtim** command to set the Delivery Traffic Indication Message (DTIM) period. The **dtim** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
dtim <value>
```

Note: The acceptable range for the dtim value is from 1 to 255 beacon intervals.

Parameters

<value>	Specifies the DTIM period in beacons

Examples

The following example sets the Delivery Traffic Indication Message period to 2 beacons.

```
EWC.enterasys.com:ap:defaults:std:radio2# dtim 2
```

4.3.6.9.9 frag

Use the **frag** command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold will be fragmented into packets that are less than or equal to this limit. The **frag** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
frag <value>
```

Parameters

<value>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery.

Examples

The following example sets the fragmentation threshold to 1500

```
EWC.enterasys.com:ap:defaults:std:radio2# frag 1500
```

4.3.6.9.10 hwretries

Use the **hwretries** command to set the number of retries for background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and turbo voice transmission queue. The **hwretries** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
hwretries (BK|BE|VI|VO|TVO) <value>
```

Parameters

BK	Specifies the number of retries for the Background transmission queue.
BE	Specifies the number of retries for the Best Effort transmission queue.
VI	Specifies the number of retries for the Video transmission queue.
VO	Specifies the number of retries for the Voice transmission queue.
TVO	Specifies the number of retries for the Turbo Voice transmission queue.

Examples

The following example sets the retry values for the background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue, and the turbo voice transmission queue as 1, 2, 3, 4, 5 respectively.

Note: You can set each parameter — background transmission queue, best effort transmission queue, video transmission queue, voice transmission queue and turbo voice transmission queue — to any value from 0 to 10 (0 means adaptive).

```
EWC.enterasys.com:ap:defaults:std:radio2# hwretries 12345
```

4.3.6.9.11 maxbrate

Use the **maxbrate** command to configure the maximum basic rate. The **maxbrate** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
maxbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps. The maximum basic rate choices adjust automatically to be higher or equal to the minimum basic rate.

Parameters

<value>	Specifies the maximum basic rate value in Mbps

Examples

The following example configures the maximum basic rate to 24 Mbps

```
EWC.enterasys.com:ap:defaults:std:radio2# maxbrate 24
```

4.3.6.9.12 max-distance

Use the **max-distance** command to set the maximum link distance, in meters, between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. If the link distance between APs is greater than the default value of 100 meters, configure the maximum distance up to 15,000 meters so that the software increases the timeout value proportionally with the distance between APs. The **max-distance** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Note: Do not change the default setting for any radio that is not participating in a Mesh or WDS.

Syntax

```
max-distance <value>
```

Parameters

<value>	Specifies the maximum distance between APs in meters. The default is 100 meters. You can enter a value from 100 to 15000 meters.

Examples

The following example sets the maximum distance between APs to 1500 meters.

```
EWC.enterasys.com:ap:defaults:std:radio2# max-distance 1500
```

4.3.6.9.13 maxoprate

Use the **maxoprate** command to set the maximum operational rate. The **maxoprate** is accessible from the **ap:defaults:std:radio2** context of the CLI.

Note: Available operational rate values (in Mbps) for Radio 2 are: 6, 9, 12, 18, 24, 36, 48, and 54.

Syntax

```
maxoprate <value>
```

Parameters

<value>	Specifies the maximum operational rate value in Mpbs

Examples

The following example sets the maximum operational rate to 24Mbps

```
EWC.enterasys.com:ap:defaults:std:radio2# maxoprate 24
```

4.3.6.9.14 minbrate

Use the **minbrate** command to configure the minimum basic rate. The **minbrate** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
minbrate <value>
```

Note: The acceptable minbrate values are 6, 12 and 24 Mbps.

Parameters

<value>	Specifies the minimum basic rate value in Mbps

Examples

The following example configures the minimum basic rate to 6 Mbps

```
EWC.enterasys.com:ap:defaults:std:radio2# minbrate 6
```

4.3.6.9.15 mode

Use the **mode** command to set the radio options for Radio 2. Use the **no** form of the command to disable Radio 2. The **mode** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
mode <b|g|bg>
```

Note: Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Parameters

b	Enables the 802.11b-only mode of Radio 2. If enabled, the AP will use only 11b (CCK) rates with all associated clients.
g	Enables the 802.11g-only mode of Radio 2. The AP will use 11g-only (OFDM) rates with all associated clients.
bg	Enables both the 802.11g mode and the 802.11b mode of Radio 2. If enabled, the AP will use 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients.

Examples

The following example enables only 802.11b mode of Radio 2.

```
EWC.enterasys.com:ap:defaults:std:radio2# mode b
```

4.3.6.9.16 pmode

Use the **pmode** command to configure the Protection Mode, which will protect 802.11g client transmissions from interruption by 802.11b clients. The **pmode** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
pmode (none|auto|always)
```

Parameters

none	Deactivates Protection Mode
auto	Indicates that Protection Mode will be used only when 802.11b clients or Wireless APs are detected
always	Indicates that Protection Mode will remain active at all times

Caution: Only use **none** if the Wireless AP will NOT be servicing 802.11b clients, and there are no 802.11b clients or Wireless APs sharing the same air space.

Examples

The following example configures the Wireless AP to use Protection Mode at all times

```
EWC.enterasys.com:ap:defaults:std:radio2# pmode always
```

4.3.6.9.17 prate

Use the **prate** command to adjust the Protection Rate. The **prate** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
prate (1|2|5.5|11)
```

Parameters

1|2|5.5|11	Specifies the Protection Rate in Mbps

Examples

The following example adjusts the Protection Rate to 5.5 Mbps

```
EWC.enterasys.com:ap:defaults:std:radio2# prate 5.5
```

4.3.6.9.18 preamble

Use the **preamble** command to set the preamble type. The **preamble** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
preamble (short|long)
```

Parameters

short	Specifies short preambles
long	Specifies long preambles

Note: For preambles set to auto, the Wireless AP will use short preambles, unless clients using the original 802.11 standard are detected.

Examples

The following example enables the long option for the preamble type

```
EWC.enterasys.com:ap:defaults:std:radio2# preamble long
```

4.3.6.9.19 ptype

Use the **ptype** command to select the Protection Type. The **ptype** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
ptype (cts only|rts cts)
```

Parameters

cts only	Specifies the Clear to Send (CTS) type
rts cts	Specifies the Request to Send (RTS) and Clear to Send (CTS) types

Examples

The following example sets the protection type to CTS

```
EWC.enterasys.com:ap:defaults:std:radio2# ptype cts only
```

4.3.6.9.20 rts

Use the **rts** command to specify the size of the Request to Send (RTS) threshold. The **rts** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Syntax

```
rts <value>
```

Note: The acceptable value for rts value is from 1 to 2346.

Parameters

<value>	Specifies the Request to Send packet size threshold.

Examples

The following example sets the RTS packet size to 256

```
EWC.enterasys.com:ap:defaults:std:radio2# rts 256
```

4.3.6.9.21 tx_max_power

Use the **tx_max_power** command to set the maximum Tx power level. The **tx_max_power** command is accessible from the **ap:defaults:std:radio2** context of the CLI.

Note: The **tx_max_power** is a maximum level when ATPC is enabled, and a fixed level when it ATPC is disabled.

Syntax

```
tx_max_power <value>
```

Parameters

<value>	Specifies the maximum Tx power level.

Examples

The following example sets the maximum Tx power level to 18 dBm.

```
EWC.enterasys.com:ap:defaults:std:radio2# tx_max_power 18
```

4.3.6.10 telnet

Use the **telnet** command to enable telnet access to the Wireless AP. Use the **no** form of the command to disable it. The **telnet** command is accessible from the **ap:defaults:std** context of the CLI.

Syntax

```
telnet
no telnet
```

Parameters

None

Examples

The following example enables telnet access to the Wireless AP

```
EWC.enterasys.com:ap:defaults:std# telnet
```

Note: After you have run the **telnet** command, you must run the **apply** command to implement the change.

4.4 export_drm

Use the **export_drm** command to export Wireless AP channel and maximum power values to an FTP server. The **export_drm** command is accessible from the **ap** context of the CLI.

Syntax

```
export_drm <server> <user> <dir> <file_name>
```

Parameters

<server>	The IP address of the FTP server on which the Wireless AP channel and maximum power values are to be uploaded.
<user>	The user name to access the FTP server
<dir>	The directory on the FTP server, where the file containing the Wireless AP channel and maximum power values are to be stored.
<file_name>	The name of the file that contains the Wireless AP channel and maximum power values.

Examples

The following example exports the DRM settings to a FTP server.

```
EWC.enterasys.com:ap# export_drm 192.168.4.211 test / drm_202.txt
Please input password:
Attempting to upload file...
SUCCESS: Upload completed.
```

Note: When the system prompts you to input password, you must type the FTP server's password.

4.5 import_drm

Use the **import_drm** command to import Wireless AP channel and maximum power values from an FTP server. The **import_drm** command is accessible from the **ap** context of the CLI.

Syntax

```
import_drm <server> <user> <dir> <file_name>
```

Parameters

<server>	The IP address of the FTP server from which Wireless AP channel and maximum power values are uploaded.
<user>	The user name to access the FTP server
<dir>	The directory on the FTP server, where the file containing the Wireless AP channel and maximum power values are stored.
<file_name>	The name of the file that contains the Wireless AP channel and maximum power values.

Examples

The following example imports the DRM settings from an FTP server

```
EWC.enterasys.com:ap# import_drm 192.168.4.163 test / exportdrm.txt
Please input password:
Attempting to download file...
SUCCESS: Download completed.
Importing 7000001222222222 - ok
Importing 0500006092051708 - ok
Importing 0500006072051287 - ok
Import DRM settings for following APs has been successful:
SN: 0500006072051287 name: 0500006072051287 radio: radio1, radio2.
SN: 0500006092051708 name: 0500006092051708 radio: radio1, radio2.
SN: 7000001222222222 name: 7000001222222222 radio: radio1, radio2.
lab-112-f:ap#
```

Note: When the system prompts you to input password, you must enter the FTP server's password.

4.6 load-groups

Use the **load-groups** refers to the **load-groups** context, which contains commands to configure Wireless AP load balancing groups. The **load-groups** command is accessible from the **ap** context of the CLI.

The following commands are available in the **ap:load-groups** context:

- create
- delete
- <named-load-group> — See <named-load-group> for commands in the **ap:load-groups:<named-load-group>** context.
- show
- maintenance

4.6.1 create

Use the **create** command to create a load group with a specified type. After creating a load group, you must assign a radio and a WLAN to the load group. See assign-radio and assign-wlan.

The **create** command is accessible from the **ap:load-groups** context of the CLI.

Syntax

```
create <load group name> [radio | client]
```

Parameters

<load group name>	The name of the load group. Load group names can be up to 32 characters long.
radio	Specifies that this load group will perform band preference steering and load control.
client	Specifies that this load group will perform client load balancing between radios. Default is client balancing

Usage

A **radio** type load group can perform band preference steering and load control. Band preference steering is a mechanism to move 11a-capable clients to the 11a radio on the AP, relieving congestion on the 11g radio. No balancing is done between the 11a and 11g radios. Load control allows you to configure the maximum number of clients allowed per radio on the AP. Load control is disabled by default. A radio load group executes band preference steering and/or load control across the radios on each AP in the group. Each AP balances in isolation from the other APs, but all APs in the group have the same configuration related to band preference and load control.

A **client** type of load group performs load balancing based on the number of clients across all APs in the group and only for the WLANs assigned to the group. This is different from load control in the **radio** type group — load control APs make decisions in isolation from each other

The number of load groups you can create is dependent on the controller you are configuring.

Table 4-1 Load Groups Supported on a Enterasys Wireless Controller

Controller	Maximum Number of Load Groups
C20	8
C20N	8
C2400	32
C4100	32
C5100	64

Each load group can contain up to 32 Wireless APs. For information about assigning a Wireless AP to a load group, see "assign-radio" on page 4-126.

Examples

The following example creates a load group named loadgroup1. This load group will be the default client balancing type.

```
EWC.enterasys.com:ap:load-groups# create loadgroup1
EWC.enterasys.com:ap:load-groups# show loadgroup1
Load Group ID: loadgroup1
Group Type: client
WLAN Assignment:
Radio Assignment:

Radio1  Radio2  AP Name

                0500008043050236
```

4.6.2 delete

Use the **delete** command to remove a load group.

The **delete** command is accessible from the **ap:load-groups** context of the CLI.

Syntax

```
delete <load group name>
```

Parameters

<load group name>	The load group being deleted.

Examples

The following example deletes the load group named loadgroup2.

```
EWC.enterasys.com:ap:load-groups# delete loadgroup2
```

4.6.3 <named-load-group>

The **<named-load-group>** command, where <named-load-group> refers to the name of a given load group, moves you into the **ap:load-groups:<named-load-group>** context, which contains commands to configure the settings of the specified individual load group.

The following commands are available in the **ap:load-groups:<named-load-group>** context. The commands available to you depends on the type of load group you are configuring, either **radio** or **client** (see create on page 4-124).

- assign-ap
- assign-radio
- assign-wlan
- bandpreference
- loadcontrol
- name
- radio-load
- show

4.6.3.1 assign-ap

Use this comment to add or remove the AP radios from the named radio type load group. The **assign-ap** command is accessible from the **ap:load-groups:<named-load-group>** context of the CLI, for load groups of type **radio**.

Syntax

```
assign-radio {add | delete} <ap-name>
```

Parameters

add | delete	Add or remove the specified AP radio from the load group.
ap-name	Specifies the AP.

Usage

If the specified AP is already assigned to a load group, a new assignment will remove the original radio assignment. You are prompted to confirm the new assignment.

Examples

This example adds a Wireless AP named AP3610_2 to named radio load group “radiogroup1.”

```
EWC.enterasys.com:ap:load-groups:radiogroup1# assign-ap add AP3610_2
```

4.6.3.2 assign-radio

Use the **assign-radio** command to assign AP radios to the named client load group. You can also use this command to unassign the AP radios from the named client load group. The **assign-radio** command is accessible from the **ap:load-groups:<named-load-group>** context of the CLI, for groups of type **client**.

Syntax

```
assign-radio (add|delete) <ap-name> (radio1|radio2|both)
```

Parameters

add|delete	Use add to assign a Wireless AP's radios to a load group. Use delete to unassign radios from a load group.
ap-name	The name of the Wireless AP
radio1|radio2|both	The radios that you want to assign or unassign.

Usage

If you assign radios that are currently assigned to another load group, the radios will automatically be removed from the other load group.

Examples

The following example assigns both radios of a Wireless AP named AP3610_2 to the client load group named clientgroup1.

```
EWC.enterasys.com:ap:load-groups:clientgroup1# assign-radio add AP3610_2 both
```

4.6.3.3 assign-wlan

Use the **assign-wlan** command to assign a WLAN service to both types of load groups. You can also use this command to unassign a WLAN service from a load group. The **assign-wlan** command is accessible from the **ap:load-groups:<named-load-group>** context of the CLI, for both types of load groups.

Syntax

```
assign-wlan (add|delete) <WLAN name>
```

Parameters

add|delete	Use add to assign a WLAN service to a load group. Use delete to unassign a WLAN service from a load group.
WLAN name	The name of the WLAN service.

Usage

You must assign a WLAN service to the load group. Assigning a WLAN service to the load group also assigns the WLAN service to the load group's Wireless APs.

Examples

The following example assigns the WLAN service named Lab45-WPA to the client load group named clientgroup1.

```
EWC.enterasys.com:ap:load-groups:clientgroup1# assign-wlan add Lab45-WPA
```

4.6.3.4 bandpreference

Use this command to enable or disable the band preference feature for all APs in a radio type load group. The **bandpreference** command is accessible from the **ap:load-groups:<named-load-group>** context of the CLI, for the radio type of load group.

Syntax

```
bandpreference <enable | disable>
```

Parameters

enable	Enable band preference steering.
disable	Disable band preference steering. The default condition is disabled.

Examples

This example enables band preference steering for the radio load group named radiogroup1.

```
EWC.enterasys.com:ap:load-groups:radiogroup1# bandpreference enable
```

4.6.3.5 loadcontrol

Use this command to enable or disable the load control per radio feature for all APs in a radio type load group. The **loadcontrol** command is accessible from the **ap:load-groups:<named-load-group>** context of the CLI, for the radio type of load group.

Syntax

```
loadcontrol <enable | disable>
```

Parameters

enable	Enable load control per radio. Use the **radio-load** command to configure the maximum number of clients per radio when load control is enabled.
disable	Disable load control per radio. The default condition is disabled. When disabled, a maximum of 121 clients is allowed for each radio.

Examples

This example enables loca control per radio for the radio load group named radiogroup1.

```
EWC.enterasys.com:ap:load-groups:radiogroup1# loadcontrol enable
```

4.6.3.6 name

Use the **name** command to change the name of a load group.The **name** command is accessible from the **ap:load-groups:<named-load-group>** context of the CLI, for both types of load groups.

Syntax

```
name <load group name>
```

Parameters

load group name	The new name of the load group

Usage

After you change the name of the load group and apply the change (with the **apply** command), the **ap:load-groups:<named-load-group>** context retains the previous name of the load group. To change the **ap:load-groups:<named-load-group>** context to the new name of the load group, you exit the context and then enter the **ap:load-groups:<named-load-group>** context using the new name.

Examples

The following example changes the name of loadgroup1 to lg_lab.

```
EWC.enterasys.com:ap:load-groups:loadgroup1# name lg_lab
EWC.enterasys.com:ap:load-groups:loadgroup1# apply
EWC.enterasys.com:ap:load-groups:loadgroup1# exit
EWC.enterasys.com:ap:load-groups# help
Available commands are:
create                          Create load group
delete                          Delete load group
end                             Return to the base mode
exit                          Return to the previous mode if not in the base mode
lg_lab                          Configure details for load group lg_lab
logout                          Exit the shell
show
EWC.enterasys.com:ap:load-groups# lg_lab
EWC.enterasys.com:ap:load-groups:lg_lab#
```

4.6.3.7 radio-load

Use this command to configure the maximum number of clients for each radio when the radio load control feature is enabled. The **radio-load** command is accessible from the **ap:load-groups:<named-load-group>** context of the CLI, for the radio type of load group.

Syntax

```
radio-load <radio1 | radio2> <max-clients>
```

Parameters

radio1 | radio2	Specifies the radio being configured.
max-clients	Specifies the maximum number of clients for the specified radio. Can be an integer between 5 and 60.

Examples

This example enables load control per radio for load group named radiogroup1, then specifies the maximum number of clients for radio 1 and radio 2.

```
EWC.enterasys.com:ap:load-groups:radiogroup1# loadcontrol enable
EWC.enterasys.com:ap:load-groups:radiogroup1# radio-load radio1 40
EWC.enterasys.com:ap:load-groups:radiogroup1# radio-load radio2 50
```

4.6.3.8 show

Use the **show** command to display information about the load group. The **show** command is accessible from the **ap:load-groups:<named-load-group>** context of the CLI, for both types of load groups.

Syntax

```
show
```

Parameters

None.

Examples

The following example displays information for the radio type load group radiogroup1.

```
EWC.enterasys.com:ap:load-groups:radiogroup1# show
Load Group ID: radiogroup1
Group Type:  radio
WLAN Assignment:

WLAN Name  Assigned

aaaa       x

Band Preference: disable
Load Control: disable
Maximum clients for radio1/radio2: 112/112
Radio Assignment:

Radio1  Radio2  AP Name

                0500008043050236
```

4.6.4 show

Use the **show** command to display a list of the load groups configured on HiPath Wireless Controller. The **show** command is accessible from the **ap:load-groups** context of the CLI.

Syntax

```
show
```

Parameters

None.

Examples

The following example displays the load groups.

```
EWC.enterasys.com:ap:load-groups# show
```

```
Load Groups:
loadgroup1
loadgroup2
```

4.7 maintenance

The **maintenance** command allows for upgrading a Wireless AP's software image. The **maintenance** command is accessible from the **ap** context of the CLI.

4.7.1 upgrd

Use the **upgrd** command to upgrade the Wireless AP's software image. The **upgrd** command is accessible from the **ap:maintenance** context of the CLI.

Syntax

```
upgrd <default|control>
```

Parameters

<default>	Specifies default upgrade. As part of the default upgrade process, when the Wireless AP registers with the controller, the AP's firmware version is verified. If it does not match with the value as defined for the default image, the AP is requested to upgrade to the default image.
<control>	Specifies controlled upgrade. The controlled upgrade allows you to individually select and control the state of a Wireless AP image upgrade. For example, you can specify which Wireless AP to upgrade, the upgrade schedule, and how to upgrade.

Examples

The following example specifies default upgrade.

```
EWC.enterasys.com:ap:maintenance# upgrd default
```

The following example specifies controlled upgrade.

```
EWC.enterasys.com:ap:maintenance# upgrd control
```

Note: After you have run the **upgrd** command to upgrade the Wireless AP's software image, you must run the **apply** command.

4.8 registration

The **registration** command refers to context **ap:registration**, which describes commands to configure registration options for connected Wireless APs.

The **registration** command is accessible from the **ap** context of the CLI.

The following commands are available in the **ap:registration** context:

- cluster-encryption
- cluster-inter-ap-roam
- cluster-shared-secret

- dinterval
- dretry
- passwd
- security
- sshpasswd

4.8.1 cluster-encryption

Use the **cluster-encryption** command to enable or disable the encryption for the cluster shared secret. The **cluster-encryption** command is accessible from the **ap:registration** context of the CLI.

Syntax

```
cluster-encryption enable | disable
```

Parameters

enable | disable	Enables or disables the encryption for the cluster shared secret.

Examples

The following example enables the encryption for the cluster shared secret.

```
EWC.enterasys.com:ap:registration# cluster-encryption enable
```

4.8.2 cluster-inter-ap-roam

Use the **cluster-inter-ap-roam** command to enable or disable cluster inter-AP roam for an AP cluster. The **cluster-inter-ap-roam** command is accessible from the **ap:registration** context of the CLI.

Syntax

```
cluster-inter-ap-roam enable | disable
```

Parameters

enable | disable	Enables or disables the

Examples

The following example enables cluster inter-AP roam.

```
EWC.enterasys.com:ap:registration# cluster-inter-ap-roam enable
```

4.8.3 cluster-shared-secret

Use the **cluster-shared-secret** command to configure the cluster shared secret. The **cluster-shared-secret** command is accessible from the **ap:registration** context of the CLI.

Syntax

```
cluster-shared-secret <string>
```

Parameters

string	The cluster shared secret, which can be 8-63 characters long.

Examples

The following example sets the cluster shared secret to “sharedsecret.”

```
EWC.enterasys.com:ap:registration# cluster-shared-secret sharedsecret
```

4.8.4 dinterval

Use the **dinterval** command to set the time delay between registration attempts. The Wireless AP will wait for a predetermined amount of time between attempts to register with the Enterasys Wireless Controller. The **dinterval** command is accessible from the **ap:registration** context of the CLI.

Syntax

```
dinterval <1-10>
```

Parameters

<1-10>	Specifies the amount of time in seconds between attempts to register with the Enterasys Wireless Controller

Examples

The following example sets the time interval between registration attempts to 6 seconds

```
EWC.enterasys.com:ap:registration# dinterval 6
```

4.8.5 dretry

Use the **dretry** command to set the number of retry attempts for the Wireless AP registration process. The Wireless AP will make a specified number of attempts to register its serial number with the Enterasys Wireless Controller following a registration failure. The **dretry** command is accessible from the **ap:registration** context of the CLI.

Syntax

```
dretry <number>
```

Parameters

<number>	Specifies the number of retry attempts for the Wireless AP registration process

Examples

The following example sets the number of registration retry attempts to 4

```
EWC.enterasys.com:ap:registration# dretry 4
```

4.8.6 passwd

Use the **passwd** command to assign a password for telnet accessible Wireless APs. The **passwd** command is accessible from the **ap:registration** context of the CLI.

For more information, see "telnet" on page 4-154.

Note: The telnet password must be between 5 and 30 alphanumeric characters.

Syntax

```
passwd <telnet password>
```

Parameters

telnet password	Specifies the telnet password.

Examples

The following example assigns password '**thisistelnetpassword**'.

```
EWC.enterasys.com:ap:registration# passwd thisistelnetpassword
```

4.8.7 security

Use the **security** command to allow only approved Wireless APs to connect to the Enterasys Wireless Controller. Use the **no** form of the command to allow all Wireless APs to connect to it. The **security** command is accessible from the **ap:registration** context of the CLI.

Note: Wireless APs without connection approval are put into a pending state, and an administrator has to manually approve those connections.

Syntax

```
security
no security
```

Parameters

None

Examples

The following example allows only approved Wireless APs to connect to the Enterasys Wireless Controller

```
EWC.enterasys.com:ap:registration# security
```

4.8.8 sshpasswd

Use the **sshpasswd** command to reset the ssh password. Use the **no** command to disable the ssh password. The **sshpasswd** command is accessible from the **ap:registration** context of the CLI.

Syntax

```
sshpasswd <password>
no sshpasswd
```

Parameters

password	Specifies the ssh password

Examples

```
EWC.enterasys.com:ap:registration# sshpasswd mynewpassword
```

Note: The password must be between 5 and 30 alphanumeric characters.

4.9 remove

Use the **remove** command to remove a client from the Wireless AP. The **remove** command is accessible from the **ap** context of the CLI.

Syntax

```
remove client (mac <MAC> | mip <MIP>)
```

Parameters

mac	Indicates that a MAC address will be specified
<MAC>	Specifies the MAC address
mip	Indicates that an IP address will be specified
<MIP>	Specifies the IP address

Examples

The following example removes a client from the Wireless AP by specifying its MAC address

```
EWC.enterasys.com:ap# remove client mac 00:12:F0:81:A4:62
```

The following example removes a client from the Wireless AP by specifying its IP address

```
EWC.enterasys.com:ap# remove client mip 172.28.209.251
```

4.10 search

Use the **search** command to search for a client on the Wireless AP by specifying its MAC address, IP Address, or User ID. The **search** command is accessible from the **ap** context of the CLI.

Syntax

```
search (mmac <MAC Address>) | (mip <IP Address>) | (muser <string>)
```

Parameters

mmac	Indicates that MAC address will be specified
<MAC>	Specifies the MAC address
mip	Indicates that an IP address will be specified
<MIP>	Specifies the IP address
muser	Indicates that a User ID will be specified
<string>	Specifies the User ID

Examples

The following example searches for a client on the Wireless AP by its MAC address

```
EWC.enterasys.com:ap# search mmac 00:12:F0:81:A4:62
00:12:F0:81:A4:62  172.28.209.251  mschap
```

The following example searches for a client on the Wireless AP by its IP Address

```
EWC.enterasys.com:ap# search mip 172.28.209.251
00:12:F0:81:A4:62  172.28.209.251  mschap
```

The following example searches for a client on the Wireless AP by specifying its User ID

```
CNL205:ap# search muser mschap
00:12:F0:81:A4:62  172.28.209.251  mschap
```

4.11 serial

Use the **serial** command to add a Wireless AP to the Enterasys Wireless Controller. The **serial** command is accessible from the **ap** context of the CLI.

Syntax

```
serial <ap serial number> <name> <hardware type> <ap role> [<description>]
```

Parameters

<ap serial number>	Specifies the serial number of the Wireless AP
<name>	Specifies a unique ID for the Wireless AP
<hardware type>	Specifies the hardware type of the Wireless AP
<ap role>	Specifies the role of the Wireless AP — whether access point or sensor.
<description>	Specifies a descriptive word for the Wireless AP

Examples

The following example adds a Wireless AP to the Enterasys Wireless Controller

```
EWC.enterasys.com:ap# serial 0409920201203751 0409920201203751-AP-Name
Orlandoe_4_P2
```

4.12 <serial>

The **<serial>** command, where <serial> refers to the serial number of a Wireless AP, moves you into the <serial> context, which contains commands to configure attributes for a specific Wireless AP. The **<serial>** command is accessible from the **ap** context of the CLI.

The following commands are available in the **ap:<serial>** context:

- leftantenna-radio2
- rightantenna-radio2
- antennaleft
- antennamiddle
- antennaright
- leftantenna-radio1
- rightantenna-radio1
- antennaleftmiddle
- antennarightmiddle
- apip
- bgway
- 802_1x — See 802_1x for commands in the **ap:<serial>:802_1x** context.
- aclist
- bcast_disassoc
- client_session
- country
- desc
- lbs-status
- led-mode
- lldp
- location
- move
- name
- persistent
- poll_timeout
- port-setting
- radio1
- radio2

- role
- show
- ssh
- telnet
- tunnel-mtu
- usedhcp
- vlanid
- wlan

4.12.1 leftantenna-radio2

Use the **leftantenna-radio2** command to select an antenna supported by the Wireless AP. Use the **help** command to list the available antenna models. Currently, this command is available for the AP2660 only. The **leftantenna-radio2** command is accessible from the **ap:<serial>** context of the CLI if the AP supports configuration of a left antenna radio2.

Syntax

```
leftantenna-radio2 <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 leftantenna-radio2 help
Error : "help" is not a valid antenna model.
Usage: leftantenna-radio2 <antenna_model>
antenna_model:
<list of valid antenna models>
No Antenna
WS-AO-2S03360 G 3.5 dBi Omni
EWC.enterasys.com:ap:0500010032150135 leftantenna-radio2 WS-AO-2S03360 G 3.5 dBi
Omni
```

This example removes a configured left radio2 antenna.

```
EWC.enterasys.com:ap:0500010032150135 leftantenna-radio2 No Antenna
```

4.12.2 rightantenna-radio2

Use the **rightantenna-radio2** command to select an antenna supported by the Wireless AP. This command is accessible from the **<serial>** context of the CLI if the AP supports configuration of a right radio2 antenna. Use the **help** command to list the available antenna models. Currently, this

command is available for the AP2660 only. The **rightantenna-radio2** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
rightantenna-radio2 <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 rightantenna-radio2 help
Error : "help" is not a valid antenna model.
Usage: rightantenna-radio2 <antenna_model>
antenna_model:
<list of valid antenna models>
No Antenna
WS-AO-2S03360 G 3.5 dBi Omni
EWC.enterasys.com:ap:0500010032150135 rightantenna-radio2 WS-AO-2S03360 G 3.5 dBi
Omni
```

This example removes a configured right radio2 antenna.

```
EWC.enterasys.com:ap:0500010032150135 rightantenna-radio2 No Antenna
dBi Omni
```

4.12.3 antennaleft

Use the **antennaleft** command to select an antenna supported by the Wireless AP. This command is accessible from the **<serial>** context of the CLI if the AP supports configuration of a left antenna. Use the **help** command to list the available antenna models. Currently, this command is available for the AP2620 and AP3620. The **antennaleft** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
antennaleft <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 antennaleft help
Error : "help" is not a valid antenna model.
Usage: antennaleft <antenna_model>
```

```
antenna_model:
<list of valid antenna models>
WS-ANT01 AG 4dBi Omni Factory
No Antenna
EWC.enterasys.com:ap:0500010032150135 antennaleft WS-ANT01 AG 4dBi Omni Factory
```

This example removes a configured left antenna.

```
EWC.enterasys.com:ap:0500010032150135 antennaleft No Antenna
```

4.12.4 antennamiddle

Use the **antennamiddle** command to select an antenna supported by the Wireless AP. This command is accessible from the **<serial>** context of the CLI if the AP supports configuration of a middle antenna. Use the **help** command to list the available antenna models. Currently, this command is available for the AP3620 only. The **antennamiddle** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
antennamiddle <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 antennamiddle help
Error : "help" is not a valid antenna model.
Usage: antennamiddle <antenna_model>
antenna_model:
<list of valid antenna models>
WS-ANT02 AG 4dBi Omni Factory
No Antenna
EWC.enterasys.com:ap:0500010032150135 antennamiddle WS-ANT02 AG 4dBi Omni Factory
```

This example removes a configured middle antenna.

```
EWC.enterasys.com:ap:0500010032150135 antennamiddle No Antenna
```

4.12.5 antennaright

Use the **antennaright** command to select an antenna supported by the Wireless AP. This command is accessible from the **<serial>** context of the CLI if the AP supports configuration of a right antenna. Use the **help** command to list the available antenna models. Currently, this command is available for the AP2620 and AP3620. The **antennaright** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
antennaright <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 antennaright help
Error : "help" is not a valid antenna model.
Usage: antennaright <antenna_model>
antenna_model:
<list of valid antenna models>
WS-ANT01 AG 4dBi Omni Factory
No Antenna
EWC.enterasys.com:ap:0500010032150135 antennaright WS-ANT01 AG 4dBi Omni Factory
```

This example removes a configured right antenna.

```
EWC.enterasys.com:ap:0500010032150135 antennaright No Antenna
```

4.12.6 leftantenna-radio1

Use the **leftantenna-radio1** command to select an antenna supported by the Wireless AP. This command is accessible from the **<serial>** context of the CLI if the AP supports configuration of a left radio1 antenna. Use the **help** command to list the available antenna models. Currently, this command is available for the AP 2660 only. The **leftantenna-radio1** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
leftantenna-radio1 <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 leftantenna-radio1 help
Error : "help" is not a valid antenna model.
Usage: leftantenna-radio1 <antenna_model>
antenna_model:
<list of valid antenna models>
WS-AO-2S03360 G 3.5 dBi Omni
No Antenna
EWC.enterasys.com:ap:0500010032150135 leftantenna-radio1 WS-AO-2S03360 G 3.5 dBi
Omni
```

This example removes a configured left radio1 antenna.

```
EWC.enterasys.com:ap:0500010032150135 leftantenna-radio1 No Antenna
```

4.12.7 rightantenna-radio1

Use the **rightantenna-radio1** command to select an antenna supported by the Wireless AP. This command is accessible from the **<serial>** context of the CLI if the AP supports configuration of a right radio1 antenna. Use the **help** command to list the available antenna models. Currently, this command is available for the AP 2660 only. The **rightantenna-radio1** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
rightantenna-radio1 <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 rightantenna-radio1 help
Error : "help" is not a valid antenna model.
Usage: rightantenna-radio1 <antenna_model>
antenna_model:
<list of valid antenna models>
WS-AO-2S03360 G 3.5 dBi Omni
No Antenna
EWC.enterasys.com:ap:0500010032150135 rightantenna-radio1 WS-AO-2S03360 G 3.5 dBi
Omni
```

This example removes a configured right radio1 antenna.

```
EWC.enterasys.com:ap:0500010032150135 rightantenna-radio1 No Antenna
```

4.12.8 antennaleftmiddle

Use the **antennaleftmiddle** command to select an antenna supported by the Wireless AP. This command is accessible from the **<serial>** context of the CLI if the AP supports configuration of a middle antenna. Use the **help** command to list the available antenna models. The **antennaleftmiddle** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
antennaleftmiddle <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 antennaleftmiddle help
Error : "help" is not a valid antenna model.
Usage: antennaleftmiddle <antenna_model>
antenna_model:
<list of valid antenna models>
WS-ANT02 AG 4dBi Omni Factory
No Antenna
EWC.enterasys.com:ap:0500010032150135 antennaleftmiddle WS-ANT02 AG 4dBi Omni
Factory
```

This example removes a configured left middle antenna.

```
EWC.enterasys.com:ap:0500010032150135 antennaleftmiddle No Antenna
```

4.12.9 antennarightmiddle

Use the **antennarightmiddle** command to select an antenna supported by the Wireless AP. This command is accessible from the **<serial>** context of the CLI if the AP supports configuration of a right antenna. Use the **help** command to list the available antenna models. The **antennarightmiddle** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
antennarightmiddle <antenna_model>
```

Parameters

<antenna_model>	Model name of an antenna supported by the Wireless AP.

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number.

```
EWC.enterasys.com:ap:0500010032150135 antennarightmiddle help
Error : "help" is not a valid antenna model.
Usage: antennarightmiddle <antenna_model>
antenna_model:
<list of valid antenna models>
WS-ANT01 AG 4dBi Omni Factory
No Antenna
EWC.enterasys.com:ap:0500010032150135 antennarightmiddle WS-ANT01 AG 4dBi Omni
Factory
```

This example removes a configured right middle antenna.

```
EWC.enterasys.com:ap:0500010032150135 antennarightmiddle No Antenna
```

4.12.10 apip

Use the **apip** command when statically configuring a Wireless AP. In order to statically configure a Wireless AP, you must first run the **no usedhcp** command. The **apip** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
apip <IP Address> <netmask>
[no] apip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameters

<IP Address>	IP address of the Wireless AP
<netmask>	Netmask of the of the Wireless AP

Examples

```
EWC.enterasys.com:ap:7000001222222222 apip 10.205.3.131 255.255.255.0
```

4.12.11 bgway

Use the **bgway** command when statically configuring a Wireless AP. In order to statically configure a Wireless AP, you must first run the **no usedhcp** command. The **bgway** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
bgway <xxx.xxx.xxx.xxx>
```

Parameters

<xxx.xxx.xxx.xxx>	Specifies the default gateway of the network.

Examples

```
EWC.enterasys.com:ap:7000001222222222 bgway 10.205.3.2
```

4.12.12 802_1x

The **802_1x** command refers to **802_1x** context that describes commands to configure 802.1x authentication for a Wireless AP. The **802_1x** command is accessible from the **ap:<serial>** context of the CLI.

The following commands are available in the **ap:<serial>:802_1x** context:

- eap
- gen_certreq
- peap

4.12.12.1 eap

Use the **eap** command to download and set the certificate from the FTP server as part of the 802.1x EAP-TLS authentication configuration process. The **eap** command is accessible from the **ap:<serial>:802_1x** context of the CLI.

Syntax

```
eap <server> <user> <dir> <file> <secret>
```

Parameters

server	IP address of the FTP server from where the certificate is to be downloaded
user	User name for accessing the FTP server
dir	The directory where the certificate is stored on the FTP server
file	The file name of the certificate
secret	The password for encrypting the private key

Examples

```
EWC.enterasys.com:Ardal AP:802_1x# eap 192.168.4.88 admin certificates ap3801.pfx
abc123
```

Note: You can use the **eap** command for EAP Proxy mode as well as EAP Pass-through mode.

4.12.12.2 gen_certreq

Use the **gen_certreq** command to generate a certificate signing request as part of the 802.1x EAP-TLS (proxy mode) authentication configuration. The **gen_certreq** command is accessible from the **ap:<serial>:802_1x** context of the CLI.

Syntax

```
gen_certreq <cn> location <country state city> organization <name, unit> email
<email_addr>]
```

Parameters

cn	Common name that you want to assign to the Wireless AP.
location	Keyword indicating that the next three parameters specify the location where the Wireless AP is operating.
country	The name of the country where the AP is located. You must use the two-letter ISO abbreviation for the country.
state	The name of the state or province where the AP is located
city	The name of the city where the AP is located
organization	Keyword indicating that the next two parameters specify the name of the organization to which the AP belongs.
name, unit	The name of the unit within the organization to which the AP belongs
email <*email_addr*>	The email address of the organization to which the AP belongs

Examples

```
EWC.enterasys.com:ap:Ardal AP:802_1x# gen_certreq shopfloor_aps location CA
Ontario Mississauga organization mnj_Ware_House Service email me@email.com
```

4.12.12.3 peap

Use the **peap** command to set PEAP (Protected Extensible Authentication Protocol) authentication. Use the **no** command to delete the PEAP authentication credentials from the Wireless AP. The **peap** command is accessible from the **ap:<serial>:802_1x** context of the CLI.

Syntax

```
peap <user> <password>
no peap
```

Parameters

None

Examples

```
EWC.enterasys.com:ap:Ardal AP:802_1x# peap admin abc123
```

4.12.13 aclist

Use the **aclist** command to statically configure the IP addresses of Enterasys Wireless Controllers for discovery. Use the **no** form of the command to remove any IPs either by address or by rank. The **aclist** command is accessible from the **ap:<serial>** context of the CLI.

Note: IP addresses removed from the Enterasys Wireless Controller list will be replaced in rank by the next listed IP address. Use the **show** function to list the added Enterasys Wireless Controller IPs by rank.

Syntax

```
aclist <IP Address>
no aclist <rank|IP Address>
```

Parameters

<Ip Address	Specifies the IP address of the Enterasys Wireless Controller
<rank>	Specifies the rank number of the listed Enterasys Wireless Controller

Examples

The following example adds three IP addresses to the Enterasys Wireless Controller list.

```
EWC.enterasys.com:ap:0409920201204003# aclist 6.178.34.54
EWC.enterasys.com:ap:0409920201204003# aclist 81.30.6.312
EWC.enterasys.com:ap:0409920201204003# aclist 167.232.92.39
```

The following example removes an entry from the Enterasys Wireless Controller list by IP address.

```
EWC.enterasys.com:ap:0409920201204003# no aclist 167.232.92.39
```

The following example removes an entry from the Enterasys Wireless Controller list by rank.

```
EWC.enterasys.com:ap:0409920201204003# no aclist 1
```

4.12.14 bcast_disassoc

Use the **bcast_disassoc** command to force the disassociation of clients from the Wireless AP. Use the **no** command to cancel the disassociation of clients from the Wireless AP. The **bcast_disassoc** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
bcast_disassoc
no bcast_disassoc
```

Parameters

None

Examples

The following example disassociates clients from the Wireless AP.

```
EWC.enterasys.com:ap:0500008043050212# bcast_disassoc
```

4.12.15 client_session

Use the **client_session** command to maintain client sessions in the event of a poll failure. Use the **no** form of the command to disable the feature. The **client_session** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
client_session
no client_session
```

Parameters

None

Examples

The following example enables user client sessions.

```
EWC.enterasys.com:ap:0500008043050212# client_session
```

4.12.16 country

Use the **country** command to specify the country in which the Wireless AP operates. The **country** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
country <country_name>
```

Parameters

<country_name>	Specifies the name of the country

Examples

The following example sets the name of the country to United States

```
EWC.enterasys.com:ap:0500008043050212# country United States
```

4.12.17 desc

Use the **desc** command to change the description of the Wireless AP. The **desc** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
desc <new_description>
```

Parameters

<new_description>	Specifies a description of the Wireless AP.

Examples

The following example provides a description for an Wireless AP

```
EWC.enterasys.com:ap:0500008043050212# desc This Access Point belongs to the Blue
Office
```

4.12.18 lbs-status

Use the **lbs-status** command to enable or disable the collection of AeroScout tags for the AP. The **lbs-status** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
lbs-status enable | disable
```

Parameters

enable|disable	Enable or disable the collection of AeroScout tags for the AP.

Examples

The following example enables the collection of AeroScout tags for the AP.

```
EWC.enterasys.com:ap:0500008043050212# lbs-status enable
```

4.12.19 led-mode

Use the **led-mode** command to configure the behavior of the Wireless AP's LEDs. The **led-mode** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
led-mode {identify | normal | off | wds-signal}
```

Parameters

identify	All LEDs blink simultaneously approximately two to four times every second.
normal	Identifies the AP status during the registration process during power on and boot process.
off	Displays fault patterns only. LEDs do not light when the AP is fault-free and the discovery is complete.
wds-signal	Indicates the WDS signal strength as a bar graph. This setting helps to align external antennas in WDS deployments by correlating the WDS link RSS with the LED pattern. Use this setting only if the AP is participating in a Mesh or WDS network.

Examples

The following example configures the LED mode to indicate WDS signal strength:.

```
EWC.enterasys.com:ap:0409920201202222# led-mode wds-signal
```

4.12.20 location

Use the **location** command to set the location string for the specified AP. The **location** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
location <location> | no location
```

Parameters

<location>	Assign an existing location or a new location
no location	Remove the location

Usage

This command supports the use of Unicode (UTF-8) strings. If the location string includes more than one word, you must enclose the string in double quotation marks.

Examples

The following example sets the location for the Wireless AP as "2nd floor south."

```
EWC.enterasys.com:ap:0500008043050236# location "2nd floor south"
EWC.enterasys.com:ap:0500008043050236# apply
EWC.enterasys.com:ap:0500008043050236# show
host_name AP3620-0500008043050236
name 0500008043050236
desc
Location: 2nd floor south
```

4.12.21 lldp

Use the **lldp** command to enable the broadcast of the LLDP protocol by a Wireless AP. Use the **no** form of the command to disable LLDP. The **lldp** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
lldp <Announcement Interval> <Announcement Delay>
no lldp
```

Parameters

<Announcement Interval>	Specifies the scheduled frequency, measured in seconds, in which the Wireless AP advertises its information by sending a new LLDP packet.
<Announcement Delay>	Specifies the delay, measured in seconds, between successive LLDP frame transmissions that is initiated by a value/status change in the LLDP local systems MIB.

Examples

The following example enables LLDP for a Wireless AP with the serial number 0409920201202222, an announcement interval of 30 seconds, and an announcement delay of 2.

```
EWC.enterasys.com:ap:0409920201202222# lldp 30 2
```

If SNMP is enabled to publish on the Enterasys Wireless Controller and you enable LLDP, the following message is displayed:

```
WARNING: SNMP is set to publish. How Do you wish to continue?
(C) Cancel
(P) Proceed
(O) Disable SNMP publishing and proceed
```

Type one of the following:

- **C** – Cancels the LLDP configuration and returns to the AP context.
- **P** – Enables LLDP and maintains SNMP running
- **O** – Enables LLDP and disables SNMP publishing

4.12.22 move

Use the **move** command to change the rank of Enterasys Wireless Controllers on the Enterasys Wireless Controller list. The **move** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
move aclist rank1 <+|-> rank2
```

Parameters

<rank1>	Specifies the rank of the listed item to be moved
<+|->	Move rank one position above or below the rank2 item
<rank2>	Specifies the rank of the second item

Examples

```
EWC.enterasys.com:ap:0500008043050212# move aclist 4 + 3
```

4.12.23 name

Use the **name** command to assign or change the name of the Wireless AP. The **name** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
name <newname>
```

Parameters

<newname>	Specifies the new name of the Wireless AP

Examples

The following example sets the name of the Wireless AP.

```
EWC.enterasys.com:ap:0500008043050212# name HomeAP1
```

4.12.24 persistent

Use the **persistent** command to enable Mode Persistence. Use the **no** form of the command to disable Mode Persistence. The **persistent** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
persistent
no persistent
```

Parameters

None

Examples

The following example enables Mode Persistence.

```
EWC.enterasys.com:ap:0500008043050212# persistent
```

The following example disables Mode Persistence.

```
EWC.enterasys.com:ap:0500008043050212# no persistent
```

Note: After you have run the **persistent** command, you must run the **apply** command to implement the changes in mode persistence.

4.12.25 poll_timeout

Use the **poll_timeout** command to set the amount of time the Wireless AP will wait for a response time from the Enterasys Wireless Controller before rebooting. The **poll_timeout** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
poll_timeout <value>
```

Note: The acceptable range for poll_timeout value is from 3 to 600.

Parameters

<value>	Specifies the amount of time in seconds to wait for a response from the Enterasys Wireless Controller before rebooting.

Examples

The following example sets the poll timeout to 10 seconds.

```
EWC.enterasys.com:ap:0500008043050212# poll_timeout 10
```

4.12.26 port-setting

Use the **port-setting** command to set the duplex mode and speed of the AP's Ethernet port. The **port-setting** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
port-setting auto|((half|full) (10 | 100))
```

Parameters

auto	Auto negotiate speed and duplex mode
half|full	Half or full duplex mode
10|100	10Mbps or 100Mbps Ethernet

Examples

The following example sets the Ethernet port on the AP to auto.

```
EWC.enterasys.com:ap:0500008043050212# port-setting auto
```

4.12.27 radio1

The **radio1** command refers to the **radio1** context, which contains commands to configure Radio 1 of the Wireless AP. The **radio1** command is accessible from the **ap:<serial>** context of the CLI.

For more information on radio1 commands, see the radio1 commands in section "defaults" on page 4-4.

4.12.28 radio2

Use the **radio2** command to configure Radio 2 of the Wireless AP. The **radio2** command is accessible from the **ap:<serial>** context of the CLI.

For more information on radio2 commands, see the radio2 commands in section "defaults" on page 4-4.

4.12.29 role

Use the **role** command to configure the role of the Wireless AP — access point or sensor. The **role** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
role (ap|sensor)
```

Parameters

(ap|sensor)	Specifies the role of the Wireless AP — access point or sensor.

Examples

The following example sets the role of the AP to sensor.

```
EWC.enterasys.com:ap:0409920201202222# role sensor
```

4.12.30 show

Use the show command to display information about the selected AP. The **show** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
show
```

Parameters

None.

Examples

The following example displays information for the AP.

```
EWC.enterasys.com:ap:0500008043050236# show
host_name AP3620-0500008043050236
name 0500008043050236
desc
Location:
role ap
ap_env indoor
usedhcp
poll_timeout 15
client_session
no persistent
```

```
no bcast_disassoc
no vlanid
country United States
led-mode normal
wlan test both
lbs-status enabled
port-setting auto
tunnel-mtu 1500
ssh enabled
antennaleft No Antenna
antennamiddle No Antenna
antennaright No Antenna
```

4.12.31 ssh

Use the **ssh** command to enable or disable SSH for the specified AP36xx AP.

The **ssh** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
ssh enable | disable
```

Parameters

enable | disable	Enables or disables SSH on the specified AP36xx AP.

Usage

The **ssh** command applies only to AP36xx APs. By default, SSH is enabled. If you disable SSH, you can still retrieve AP traces from the controller through SFTP.

Examples

The following command disables SSH on AP 0500008043050236.

```
EWC.enterasys.com:ap:0500008043050236# ssh disable
```

4.12.32 telnet

Use the **telnet** command to enable telnet access to the Wireless AP. Use the **no** form of the command to disable it. The **telnet** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
telnet
no telnet
```

Parameters

None

Examples

The following example enables telnet access to the Wireless AP.

```
EWC.enterasys.com:ap:0409920201204003# telnet
```

4.12.33 tunnel-mtu

Use the **tunnel-mtu** command to set the static MTU value. The **tunnel-mtu** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

tunnel-mtu <600-1500>

Parameters

<600-1500>	Specifies the static MTU size in bytes. The default is 1500 bytes.

Usage

The Enterasys wireless software enforces the static MTU size if it cannot discover the MTU size. Set the MTU size to allow the source to reduce the packet size and avoid the need to fragment data packets in the tunnel.

Examples

The following command sets the MTU tunnel size to 1300 bytes..

```
EWC.enterasys.com:ap:0500008043050236# tunnel-mtu 1300
```

4.12.34 usedhcp

Use the **usedhcp** command to enable DHCP. Use the **no** form of the command to statically configure a Wireless AP. The **usedhcp** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
usedhcp
no usedhcp
```

Parameters

None

Examples

The following example enables DHCP on the Enterasys Wireless Controller.

```
EWC.enterasys.com:ap:0122003880188015# usedhcp
```

4.12.35 vlanid

Use **vlanid** to assign a VLAN tag to the subnet carrying the Wireless AP's management traffic. The **vlanid** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
vlanid <1-4094>
```

Parameters

<1-4094>	Specifies the ID tag for the VLAN

Examples

The following example assigns the subnet a VLAN tag.

```
EWC.enterasys.com:ap:0122003880188015# vlanid 4
```

4.12.36 wlan

Use the **wlan** command to assign one or both of the AP's radios to the specified WLAN service. You can also use this command to unassign the AP's radios from the specified WLAN service. The **wlan** command is accessible from the **ap:<serial>** context of the CLI.

Syntax

```
wlan <wlans name> (radio1|radio2|both|none)
```

Parameters

<wlans name>	The WLAN service to which you want to assign the AP's radios or from which you want to unassign the AP's radios.
(radio1|radio2|both|none)	Specifies the radios that you want to assign to the WLAN service. Use **none** to unassign the radios from the WLAN service.

Examples

The following example assigns radio 2 of AP 0500008043050355 to the WLAN service named CNL-91-0-1.

```
EWC.enterasys.com:ap:0500008043050355# wlan CNL-91-0-1 radio2
EWC.enterasys.com:ap:0500008043050355# show
host_name AP3605-0500008043050355
name AP3605 internal
desc
usedhcp
poll_timeout 15
client_session
no persistent
no bcast_disassoc
no vlanid
country Germany
```

```
led-mode normal
wlan CNL-91-0-1 radio2
```

5

checkpoint Commands

The Enterasys Wireless Controller forwards specified event messages to an ELA server using Check Point software's OPSEC ELA protocol. The server tracks and analyzes these event messages and forwards suspicious information to a firewall application.

This section describes commands which enable and configure Check Point event logging options for the Enterasys Wireless Controller. These commands are located in the **checkpoint** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **checkpoint** context:

- cpip
- cplog
- cpcert
- elalogint
- elaport
- elaq
- elaretry
- sicname
- sicpwd

5.1 cpip

Use the **cpip** command to set the IP address of the ELA Management Station.

Suspicious messages tracked by the ELA server are sent to the firewall of the ELA Management Station.

Note: You must enable checkpoint logging before this command will become visible in the CLI. For more information, see "cplog" on page 5-2.

Syntax

```
cpip <IP Address>
```

Parameters

<IP Address>	Specifies the IP address of the ELA Management Station

Examples

The following example sets the IP address of the ELA Management Station.

```
EWC.enterasys.com:checkpoint# cpip 134.127.56.9
```

5.2 cplog

The Wireless Controller forwards specified event messages to an Event Logging Application Program Interface (ELA) server, which tracks and analyzes messages and forwards suspicious content to a firewall.

Use the **cplog** command to enable Check Point Logging, with optional parameters to specify the IP address, port, logging queues and logging delays of the Check Point server. Use the **no** form of the command to disable it.

Syntax

```
cplog [<IP Address> <elaport> <elalogint> <elaretry> <elaq> <sicname> <sicpwd>]
no cplog
```

Parameters

<IP Address>	Specifies the IP address of the ELA management station, where suspicious messages tracked by the ELA server are sent
<elaport>	Specifies the ELA port
<elalogint>	Specifies the amount of time (in milliseconds) system waits before attempting to log
<elaretry>	Specifies the amount of time (in milliseconds) the system waits before attempting to reconnect.
<elaq>	Specifies the number of messages the log queue holds if the controller and Check Point gateway become disconnected
<sicname>	Specifies the Secure Internal Communication name, which serves as a security-based ID
<sicpwd>	Specifies the Secure Internal Communication password

Examples

The following example enables Check Point logging and sets the necessary parameters.

```
EWC.enterasys.com:checkpoint# cplog 192.103.12.1 131 90 3001 999 name1 pass
```

To view changes made to the system, the **show** command is used for each parameter

```
EWC.enterasys.com:checkpoint# show cpip
EWC.enterasys.com:checkpoint# show elaport
EWC.enterasys.com:checkpoint# show elalogint
EWC.enterasys.com:checkpoint# show elaretry
```

```
EWC.enterasys.com:checkpoint# show elaq
EWC.enterasys.com:checkpoint# show sicname
EWC.enterasys.com:checkpoint# show sicpwd
```

5.3 cpcert

Use the **cpcert** command to generate a certificate to be sent to the ELA Management Station.

Syntax

```
cpcert
```

Parameters

None

Examples

The following example generates a certificate

```
EWC.enterasys.com:checkpoint# cpcert
```

5.4 elalogint

When a connection between the Enterasys Wireless Controller and the Check Point gateway is established, the system will wait for a certain amount of time before it begins to create logs.

Use the **elaglogint** command to set the amount of time (in milliseconds) the system should wait before attempting to write log messages.

Syntax

```
elalogint <value>
```

Parameters

<value>	The time in milliseconds the system will wait before logging messages.

Examples

The following example sets the log interval time to 4 ms.

```
EWC.enterasys.com:checkpoint# elalogint 4
```

5.5 elaport

Use the **elaport** command to set the Event logging Application Program Interface (API) port for Check Point logging.

Note: The **cpip**, **sicname**, and **sicpwd** values must also be set before the **apply** command can be used.

Syntax

```
elaport <value>
```

Parameters

<value>	Specifies the Event Logging API port

Examples

The following example sets the elaport value to port 999.

```
EWC.enterasys.com:checkpoint# elaport 999
```

5.6 elaq

If the Enterasys Wireless Controller and the Check Point gateway become disconnected, any event log messages are placed into a queue.

Use the **elaq** command to set the size of the Event Logging (ELA) API queue.

Syntax

```
elaq <value>
```

Parameters

<value>	Specifies the number of log entries the ELA queue will hold

Examples

The following example sets the ELA queue size to 600

```
EWC.enterasys.com:checkpoint# elaq 600
```

5.7 elaretry

The system will wait for a predetermined time before attempting to reconnect the Enterasys Wireless Controller and the Check Point gateway.

Use the **elaretry** command to set the ELA Retrial Interval.

Syntax

```
elaretry <value>
```

Parameters

<value>	Specifies the time interval (in milliseconds) the system will wait before attempting to reconnect the controller and the Check Point gateway

Examples

The following example sets the ELA Retrial Interval to 714 ms.

```
EWC.enterasys.com:checkpoint# elaretry 714
```

5.8 sicname

Use the **sicname** command to set the Secure Internal Communication (SIC) name, which serves as the security-based ID.

Syntax

```
sicname <string>
```

Parameters

<string>	Specifies the Secure Internal Communication name

Examples

The following example sets the SIC name

```
EWC.enterasys.com:checkpoint# sicname JohnDoe
```

5.9 sicpwd

Use the **sicpwd** command to set the Secure Internal Communication (SIC) password.

Syntax

```
sicpwd <string>
```

Parameters

<string>	Specifies the Secure Internal Communication password

Examples

The following example sets the SIC password

```
EWC.enterasys.com:checkpoint# sicpwd secret123
```

6

l2ports Commands

This section describes commands to enable and disable ports on the Enterasys Wireless Controller. These commands are located in the **l2ports** context of the CLI. L2 port configuration is performed within a named topology context. See "l2" on page 21-5 for L2 port configuration information.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **l2ports** context:

- esaN
- pc.N
- portN
- show

6.1 esaN

The **esaN** command moves you into the context **l2ports:esaN** (where variable **N** refers to the physical data port number). This context contains the port command which enables or disables ports. This command is available on the following controllers: CRBT8110, CRBT8210, C20, C2400, and C5110. See "port" on page 6-2 for information on enabling and disabling a port in this context.

6.2 pc.N

The **pc.N** command moves you into the context **l2ports:pc.N** (where variable **N** refers to the physical data port number). This context contains the port command which enables or disables ports. This command is available on the C20N controller. See "port" on page 6-2 for information on enabling and disabling a port in this context.

6.3 portN

The **portN** command moves you into the context **l2ports:portN** (where variable **N** refers to the physical data port number). This context contains the port command which enables or disables

ports. This command is available on the C4110 platform. See “port” on page 6-2 for information on enabling and disabling a port in this context.

6.3.1 port

Use the **port** command to enable or disable the port from within the appropriate port context for your platform:

- **l2ports:esaN#** is available on the CRBT8110, CRBT8210, C20, C2400, and C5110 controllers. See “esaN” on page 6-1.
- **l2ports:pc.N#** is available on the C20N controller. See “pc.N” on page 6-1.
- **l2ports:portN#** is available on the C4110 controller. See “portN” on page 6-1.

Syntax

```
port enable | disable
```

Parameters

enable	Enables the port for this context.
disable	Disables the port for this context.

Examples

The following example enables the ESA1 port in an **l2ports:esa1#** context:

```
EWC.enterasys.com# l2ports
EWC.enterasys.com:l2ports# esa1
EWC.enterasys.com:l2ports:esa1# port enable
EWC.enterasys.com:l2ports:esa1# apply
EWC.enterasys.com:l2ports:esa1# show
Port: enable
EWC.enterasys.com:l2ports:esa1#
```

6.4 show

Use the **show** command in the **l2ports** context to display port information for the Enterasys Wireless Controller.

Syntax

```
show
```

Parameters

None

Examples

The following example displays port information for the Enterasys Wireless Controller:

```
EWC.enterasys.com# l2ports
EWC.enterasys.com:l2ports# show
Status  Enable  Port   MAC               VLAN Physical  VLAN Service
UP      enable  esa0   08:00:06:81:C2:AD  625            527,626
DOWN    enable  esa1   08:00:06:81:C2:AE  4094
DOWN    enable  esa2   08:00:06:81:C2:AF  -1
DOWN    enable  esa3   08:00:06:81:C2:B0  -1
UP      enable  admin  08:00:06:85:91:A7
```

Note: The VLAN Service field specifies the VLAN IDs set on bridged at controller topologies for the specific physical port (in this case esa0).

7

ip Commands

This section describes the commands with options to configure routing information. These options can be found within the **ip** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **ip** context:

- route
- ospf — See ospf for commands in the **ip:ospf** context.

7.1 route

Use the **route** command to add routing information. Use the **no** forms of the command to disable the information.

Note: Use **show routes** to display the routing table. For more information, see “show routes” on page 3-50.

Syntax

```
route <IP Address>/<netmask> <gateway> [float|nofloat]
route <IP Address> <netmask> <gateway> [float|nofloat]
route default <gateway> [float|nofloat]
no route <IP Address>/<netmask>
no route <IP Address> <netmask>
no route default
no route <routeId>
```

Parameters

<IP Address>	Specifies the destination IP address
<netmask>	Specifies the subnet mask
/<netmask>	Specifies the subnet mask in CIDR format
<gateway>	Specifies the gateway
float	Does not override Open Shortest Path First (OSPF) learned route
nofloat	Overrides OSPF learned route

<routeId>	Specifies index number of route on the routing table

Examples

The following example adds an IP address to the routing table, specifying the netmask in CIDR format and disallowing OSPF overrides

```
EWC.enterasys.com:ip# route 1.1.2.1/24 10.7.0.3 nofloat
```

The following example adds an IP address to the routing table, specifying the netmask as an IP address and allowing OSPF overrides

```
EWC.enterasys.com:ip# route 1.1.2.1 255.255.255.0 10.7.0.3 float
```

The following example configures the default route

```
EWC.enterasys.com:ip# route default 10.7.0.3
```

The following example removes an IP address from the routing table and indicates the netmask by size

```
EWC.enterasys.com:ip# no route 1.1.2.1/24
```

The following example removes an IP address from the routing table and indicates the netmask by IP address.

```
EWC.enterasys.com:ip# no route 1.1.2.1 255.255.255.0
```

The following example removes the default route from the routing table

```
EWC.enterasys.com:ip# no route default
```

The following example removes an IP address from the routing table by its index number

```
EWC.enterasys.com:ip# no route 12
```

7.2 ospf

The **ospf** command is associated with the context **ip:ospf**, which contains commands to configure global settings for the Open Shortest Path First (OSPF) protocol on a network.

The following commands are available in the **ip:ospf** context.

- area
- areatype
- routerid
- status
- ospfinterface — See ospfinterface for commands in the **ip:ospf:ospfinterface** context.

7.2.1 area

Use the **area** command to define the area identification of the OSPF interface.

Syntax

```
area <area_id>
```

Parameters

<area_id>	Specifies an integer or an IP address defining the OSPF area

Examples

The following example sets the OSPF area to Area 0.

```
EWC.enterasys.com:ip:ospf# area 0.0.0.0
```

7.2.2 areatype

Use the **areatype** command to select the type of Open Shortest Path First (OSPF) protocol area to be used on the Enterasys Wireless Controller.

Syntax

```
areatype (default|stub|nssa)
```

Parameters

default	Selects the Normal OSPF area
stub	Selects the Stub area
nssa	Selects the "Not So Stubby" area

Examples

The following example sets the OSPF area type to a Stub area

```
EWC.enterasys.com:ip:ospf# areatype stub
```

7.2.3 routerid

Use the **routerid** command to identify the IP address of the router originating Open Shortest Path First (OSPF) packets.

Syntax

```
routerid <IP Address>
```

Parameters

<IP Address>	Specifies the IP address of the router originating OSPF packets

Examples

The following example sets the routerid to 1.1.1.1

```
EWC.enterasys.com:ip:ospf# routerid 1.1.1.1
```

7.2.4 status

Use the **status** command to enable or disable the Open Shortest Path First (OSPF) protocol on the Enterasys Wireless Controller.

Syntax

```
status (enable|disable)
```

Parameters

enable	Indicates that the OSPF will be enabled
disable	Indicates that the OSPF will be disabled

Examples

The following example enables OSPF on the Enterasys Wireless Controller

```
EWC.enterasys.com:ip:ospf# status enable
```

7.2.5 ospfinterface

The **ospfinterface** command moves you to the context **ip:ospf:ospfinterface**, which contains commands to configure Open Shortest Path First (OSPF) protocol options for a port of the Enterasys Wireless Controller. The **ospfinterface** command supports the specifying of an esa**N** interface, where **N** is a number from 0 - 3. For example, the command **ospfinterface 1** moves you to the OSPF interface esa1 (**ip:ospf:ospfinterface:1**) configuration context.

The **ospfinterface** command is accessible from within the **ip:ospf** context.

The following commands are available in the **ip:ospf:ospfinterface** context.

- <n>
- authkey
- authtype
- deadinterval
- hellointerval
- linkcost
- retransmitinterval
- status
- transmitdelay

7.2.5.1 <n>

Use the **<n>** command, where **n** is a number from 0 - 3, to move to the **ip:ospf:ospfinterface:N** context for the configuration of the OSPF esa**N** interface.

The **<n>** command is accessible from within the **ip:ospf:ospfinterface** context.

Syntax

```
<n>
```

Parameters

None.

Examples

The following moves you to the **ip:ospf:ospfinterface:0** context for the configuration OSPF interface esa0.

```
EWC.enterasys.com:ip:ospf:ospfinterface# 0
EWC.enterasys.com:ip:ospf:ospfinterface:0#
```

7.2.5.2 authkey

Use the **authkey** command to set the password used for authentication. Use the **no** form of the command to clear the password.

Note: Authentication must be configured to use a password before this command can be used. For more information, see “authtype” on page 7-5.

Syntax

```
authkey <password>
no authkey
```

Parameters

<password>	Specifies the password used for authentication

Examples

The following example sets an authentication password

```
EWC.enterasys.com:ip:ospf:ospfinterface:0# authkey hello123
```

7.2.5.3 authtype

Use the **authtype** command to indicate whether the authentication will require a password or not.

Syntax

```
authtype (none|password)
```

Parameters

none	Indicates that no password is required
password	Indicates that authentication will require a password

Examples

The following example configures authentication to require a password

```
EWC.enterasys.com:ip:ospf:ospfinterface:0# authtype password
```

7.2.5.4 deadinterval

Use the **deadinterval** command to set the amount of time the OSPF protocol will wait for a response before assuming peer devices are unreachable.

Syntax

```
deadinterval <1-65535>
```

Parameters

<1-65535>	Specifies the time interval (in seconds) the OSPF protocol will wait for a response

Examples

The following example sets the time to wait for a packet response to 300 seconds

```
EWC.enterasys.com:ip:ospf:ospfinterface:0# deadinterval 300
```

7.2.5.5 hellointerval

Use the **hellointerval** command to specify the time interval between the transmission of OSPF Hello packets to devices on the network.

Syntax

```
hellointerval <1-65535>
```

Parameters

<1-65535>	Specifies a time interval in seconds

Examples

The following example sets the time interval between outgoing packets to 10 seconds

```
EWC.enterasys.com:ip:ospf:ospfinterface:0# hellointerval 10
```

7.2.5.6 linkcost

Use the **linkcost** command to assign a Link Cost to the port.

Syntax

```
linkcost <1-65535>
```

Parameters

<1-65535>	Specifies a numerical value

Examples

The following example sets the Link Cost of the port to 10

```
EWC.enterasys.com:ip:ospf:ospfinterface:0# linkcost 10
```

7.2.5.7 retransmitinterval

Use the **retransmitinterval** command to set the amount of time the port will wait before it attempts to retransmit outgoing packets

Syntax

```
retransmitinterval <1-65535>
```

Parameters

<1-65535>	Specifies the time interval in seconds

Examples

The following example sets the retransmission time interval to five seconds

```
EWC.enterasys.com:ip:ospf:ospfinterface:0# retransmitinterval 5
```

7.2.5.8 status

Use the **status** command to enable or disable OSPF advertising on the port.

Syntax

```
status (enable|disable)
```

Parameters

enable	Indicates that OSPF advertising will be enabled
disable	Indicates that OSPF advertising will be disabled

Examples

The following example enables OSPF advertising on the port

```
EWC.enterasys.com:ip:ospf:ospfinterface:0# status enable
```

7.2.5.9 transmitdelay

Use the **transmitdelay** command to set the delay time before initiating transmission.

Syntax

```
transmitdelay <1-65535>
```

Parameters

<1-65535>	Specifies the amount of time in seconds

Examples

The following example sets the delay time for transmission to one second

```
EWC.enterasys.com:ip:ospf:ospfinterface:0# transmitdelay 1
```

8

login Commands

The **login** command refers to **login** context, which contains commands to configure the login authentication modes. The **login** command is accessible from the root context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The Enterasys Wireless Controller offers four login authentication options:

- Local authentication
- RADIUS-based authentication
- Local authentication first, then RADIUS-based authentication
- RADIUS-based authentication first, then local authentication

Local authentication is enabled by default. If the administrator chooses to use the RADIUS-based login, all password policy enforcement is delegated to the RADIUS server, and the account management features on the CLI are disabled.

You must test the RADIUS server configuration before configuring a user profile (User ID and Password), and submitting it to the RADIUS server.

After you have switched to RADIUS-based login, you must use the RADIUS credentials to log on the Enterasys Wireless Controller.

The following commands are available in the **login** context.

- apply
- auth — See auth for commands in the **login:auth** context.
- auth-order
- move
- show

8.1 apply

Use the **apply** command to save login configuration changes.

Syntax

```
apply
```

Parameters

None

Examples

The following example saves login configuration changes.

```
EWC.enterasys.com:login# apply
```

8.2 auth

The **auth** command moves you into the **login:auth** context, which contains commands to configure the RADIUS server for RADIUS-based login.

The following commands are available in the **login:auth** context.

- server
- primary
- authset
- move
- radtest_login

8.2.1 server

Use the **server** command to select a RADIUS server. The **server** command is available from the **login:auth** context.

Syntax

```
server (<#>|<name>)
no server (<#>|<name>)
```

Parameters

<#>	Specifies the index number of the RADIUS server to be used
<name>	Specifies the name of the RADIUS server to be used

Examples

The following example selects a radius server by name

```
EWC.enterasys.com:login:auth# server rad2
```

8.2.2 primary

Use the **primary** command to set the RADIUS server as the primary server for authentication. Use the **no** form of the command to disable it. The **primary** command is available from the **login:auth** context.

Syntax

```
primary <server_name>
no primary <server_name>
```

Parameters

<server_name>	Specifies the name of the server

Examples

The following example sets the primary authentication server

```
EWC.enterasys.com:login:auth# primary FreeRadius70
```

8.2.3 authset

Use the **authset** command to set authentication server information. The **authset** command is available from the **login:auth** context.

Syntax

```
authset <server_name> <port> <retry_value> <time_out> <nas_ip> <nas_string>
<PAP|CHAP|MS-CHAP|MS-CHAP2>
```

Parameters

<server_name>	Specifies a valid RADIUS server name
<port>	Specifies the RADIUS server port
<retry_value>	Specifies the number of times to attempt to access the RADIUS server
<time_out>	Specifies the time in seconds to wait for a response from the RADIUS server before trying again
<NAS_IP>	Specifies the NAS IP address
<nas_string>	Specifies the Network Access Server (NAS) Identifier
<PAP | CHAP | MS-CHAP | MS-CHAP2>	Specifies the Authentication Protocol

Examples

The following example specifies the authentication server information.

```
EWC.enterasys.com:login:auth# authset Radius 1812 3 5 192.168.4.112 NAS MS-CHAP
```

8.2.4 move

Use the **move** command to change the order of the RADIUS server in the list of RADIUS servers. The **move** command is available from the **login:auth** context.

Syntax

```
move <#1> {+|-} <#2>
```

Parameters

<#1>	Specifies Server # 1 in the list of RADIUS servers
{+}	Specifies to move the RADIUS server up in order
{-}	Specifies to move the RADIUS server down in order

<#2>	Specifies Server # 2 in the list of RADIUS servers

Examples

The following example moves the Server # 1 to second in order in the list of RADIUS servers.

```
EWC.enterasys.com:login:auth# move #1 -
```

8.2.5 radtest_login

Use the **radtest_login** command to check the RADIUS server's configuration. The **radtest_login** command is available from the **login:auth** context.

Syntax

```
radtest_login <user name> <password>
```

Parameters

user name	User Name required to log on the controller
password	Password required to log on the controller

Examples

The following example tests the RADIUS server's configuration.

```
EWC.enterasys.com:login:auth# radtest_login admin abc123
==> called pam_start (1)
got success
==> called pam_authenticate
got: 'Success'
RETURN VALUE: 0 resp.code: 0
Test Result: Success
```

8.3 auth-order

Use the **auth-order** command to add an authentication mode to the end of the ordered list of authentication modes. You can also delete an authentication mode from the ordered list.

Syntax

```
auth-order <add|delete> <radius|local>
```

Parameters

<add|delete>	Specifies whether an authentication mode is to be added to or deleted from the ordered list.
<radius|local>	Specifies authentication mode to be added or deleted

Usage

- You must configure the RADIUS server before you can add RADIUS-based authentication to the list. To do this, use the **auth** commands. See auth.
- You cannot add duplicate authentication modes to the list.
- The authentication order list must contain at least one authentication mode. You cannot delete an authentication mode if it is the only mode in the list.
- To change the order of authentication modes in the list, use the **move** command. See move

Examples

The following example sets the login authentication to RADIUS-based mode.

```
EWC.enterasys.com:login# auth-order add radius
EWC.enterasys.com:login# auth-order delete local
Changing login mode will cause CLI to terminate. Do you want to proceed? y|[n]:y
************************************************************
  Login mode has changed. CLI will terminate in 5 seconds!
************************************************************
```

The following example sets the login authentication to the combination of local authentication first, then RADIUS-based authentication.

```
EWC.enterasys.com:login# show
1 authentication method: local
EWC.enterasys.com:login# auth-order add radius
EWC.enterasys.com:login# show
1 authentication method: local
2 authentication method: radius
```

8.4 move

Use the **move** command to change the order of authentication modes in the authentication mode ordered list.

Syntax

```
move <order> <order>
```

Parameters

<order>	Specifies the current priority of the authentication mode.

Usage

Use the **show** command to view the priorities of the authentication modes. See show.

Examples

The following example changes the authentication mode order from local, RADIUS to RADIUS, local.

```
EWC.enterasys.com:login# show
```

```
1 authentication method: local
2 authentication method: radius
EWC.enterasys.com:login# move 2 1
EWC.enterasys.com:login# show
1 authentication method: radius
2 authentication method: local
EWC.enterasys.com:login# apply
Changing login mode will cause CLI to terminate. Do you want to proceed? [y|n]:y
************************************************************
  Login mode has changed. CLI will terminate in 5 seconds!
************************************************************
```

8.5 show

Use the **show** command to display the currently configured authentication modes and their priorities.

Syntax

```
show
```

Parameters

None

Examples

```
EWC.enterasys.com:login# show
1 authentication method: local
```

9

mitigator Commands

The Enterasys Wireless Controller uses a mechanism known as the Mitigator to assist in the detection of rogue Access Points.

The Mitigator function has three main components: an RF scanning task that runs on the Wireless AP, an RF Data Collector (RFDC) to receive and manage RF scan messages sent by the Wireless AP, and an Analysis Engine to process data from the RFDC.

This section describes the commands that enable and configure the Mitigator options for the controller. These commands are located in the **mitigator** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **mitigator** context:

- analysis
- wcswip
- scgroup — See scgroup for commands in the **mitigator:scgroup** context.
- friend

9.1 analysis

Use the **analysis** command to enable the Mitigator Analysis Engine. Use the **no** form of the command to disable it. The **analysis** command is accessible from the **mitigator** context of the CLI.

Syntax

```
analysis
no analysis
```

Parameters

None

Examples

The following command enables the Mitigator Analysis Engine.

```
EWC.enterasys.com:mitigator# analysis
```

Note: After you have enable or disable the Mitigator Analysis Engine, you must run the **apply** command to implement the changes.

9.2 wcswip

Use the **wcswip** command to set the IP address of a Remote Data Collection Engine. Use the **no** format of the command to remove the IP address.

Syntax

```
wcswip <IP Address> [<poll_interval(3-60)> <retries(0-12)>]
no wcswip <IP Address>
```

Parameters

IP Address	Specifies the IP address of the Remote Data Collection Engine
poll_interval	Specifies the time interval (in seconds) that the Analysis Engine will poll the Remote Data Collection Engine. The values from 3 to 60 are accepted.
retries	Specifies the number of times the Analysis Engine will attempt to poll the Remote Data Collection Engine to maintain connection status before it stops sending requests. The values from 0 to 12 are accepted.

Examples

The following example sets the IP address of the Data Collection Engine and the required intervals, and then applies the changes.

```
EWC.enterasys.com:mitigator# wcswip 123.456.789.101 3 1
```

Note: After you have set the IP address of a Remote Data Collection Engine, you you must run the **apply** command to implement the changes.

To verify that the change has been made, use the **show** command

```
EWC.enterasys.com:mitigator# show wcswip
```

To remove the IP address, the **no** form of the command is used, followed by the **apply** command to implement the change.

```
EWC.enterasys.com:mitigator# no wcswip 123.456.789.101
```

9.3 scgroup

The **scgroup** command refers to context scgroup, which contains commands to create and delete the scan groups. The **scgroup** command is accessible from the **mitigator** context of the CLI.

The following commands are available in the **mitigator:scgroup** context:

- sgname
- <scan group name> — See <scan group name> for commands in the **mitigator:scgroup:<scan group name>** context.

9.3.1 sgname

Use the **sgname** command to create a scan group. Use the **no** form of the command to delete the scan group. The **sgname** command is accessible from the **mitigator:scgroup** context of the CLI.

Syntax

```
sgname <scan group name> <10-120> [dtime <1-1000>] [radio1 |radio2|both] [channel all|current] [type active|passive] [serial <serial>...]
no sgname <scan group name>
```

Parameters

scan group name	Specifies the scan group name
10-20	Specifies the scan time interval
dtime <1-1000>	Specifies the Channel Dwell Time of the scan group
radio1 | radio2 | both	Specifies radios — radio 1, radio 2, or both
channel all | current	Specifies the channels to be scanned — all or current
type active | passive	Specifies the scan type — active or passive
serial	Specifies to add the Wireless APs by their serial numbers to the scan group.
<serial>	Specifies the serial number of the Wireless APs that are to be added to the scan group

Examples

The following example creates a scan group named South-Block.

```
EWC.enterasys.com:mitigator:scgroup# sgname South-Block 100 dtim 300 radio both channel all type active serial 0500006072051354 0500006072051427 0500006062051048 0500006062051040
```

Note: After you have added the Wireless APs to the scan group, you must run the **apply** command to implement the changes.

9.3.2 <scan group name>

The **<scan group name>** is a context, which contains commands to modify the attributes for a specified scan group, where the parameter **<scan group name>** refers to the scan group's name.

The **<scan group name>** command is accessible from the **mitigator:scgroup** context of the CLI.

The following commands are available in the the **mitigator:scgroup:<scan group name>** context:

- aplist
- interval
- dtime
- radio
- type
- channel
- start

- show

9.3.2.1 aplist

Use the **aplist** command to modify the list of the Wireless AP that are part of the scan group. Use the **no** form of the command to delete the Wireless APs from the list.

Syntax

```
[no] aplist <serial>...
aplist <serial>...
```

Parameters

<serial...>	Specifies the Wireless AP by their serial numbers that are to be added to the scan group

Examples

The following example adds the Wireless APs of the following serial numbers to the scan group: 500006072051354 and 0500006072051427.

```
EWC.enterasys.com:mitigator:scgroup:South Block# aplist 500006072051354
0500006072051427
```

Note: After you have run the **aplist** command, you must run the **apply** command to start the scanning.

9.3.2.2 interval

Use the **interval** command to modify the scan time interval in minutes. Valid values are from 10 to 120 minutes.

Syntax

```
interval <period>
```

Parameters

<period>	Specifies the scan time interval period in minutes

Examples

The following example modifies the scan time interval to 30 minutes.

```
EWC.enterasys.com:mitigator:scgroup:South Block# interval 30
```

Note: After you have run the **interval** command, you must run the **apply** command to start the scanning.

9.3.2.3 dtime

Use the **dtime** command to modify the Channel Dwell Time of the scan group.

Syntax

```
dtime <1-1000>
```

Parameters

None

Examples

The following example sets the channel dwell time of scan group South Block to 100 milliseconds.

```
EWC.enterasys.com:mitigator:scgroup:South Block# dtime 100
```

Note: After you have run the **dtime** command, you must run the **apply** command to start the scanning.

9.3.2.4 radio

Use the **radio** command to modify the radio mode to be used for scanning.

Syntax

```
radio <radio1|radio2|both>
```

Parameters

radio1	Specifies radio 1 to be used
radio2	Specifies radio 2 to be used
both	Specifies both radio 1 and radio 2

Examples

The following example sets radio 1 to be used.

```
EWC.enterasys.com:mitigator:scgroup:South Block# radio1
```

Note: After you have run the **radio** command, you must run the **apply** command to start the scanning.

9.3.2.5 type

Use the **type** command to modify the scan type — active or passive.

Syntax

```
type active|passive
```

Parameters

active	Specifies active type scanning
passive	Specifies passive type scanning

Examples

The following example sets the scan type to active.

```
EWC.enterasys.com:mitigator:scgroup:South Block# type active
```

Note: After you have run the **type** command, you must run the **apply** command to start the scanning.

9.3.2.6 channel

Use the **channel** command to modify the **Channel List** — scanning on all channels or on the current channels.

Syntax

```
channel all|current
```

Parameters

all	Specifies all channels to be scanned
current	Specifies the current channel to be scanned

Examples

The following example sets the current channel to be scanned.

```
EWC.enterasys.com:mitigator:scgroup:South Block# channel current
```

Note: After you have run the **channel** command, you must run the **apply** command to start the scanning.

9.3.2.7 start

Use the **start** command to start the scanning.

Syntax

```
start
```

Parameters

None

Examples

The following example starts the scanning.

```
EWC.enterasys.com:mitigator:scgroup:South-Block# start
```

Note: After you have run the **start** command, you must run the **apply** command to start the scanning.

9.3.2.8 show

Use the **show** command to display the scan groups's settings.

Syntax

```
show
```

Parameters

None

Examples

The following example displays the scan group South Block's settings.

```
EWC.enterasys.com:mitigator:scgroup:South-Block# show
Interval 100
dtime 300
radio both
channel current
type active
serial 0500006072051354 0500006072051427 0500006062051048 0500006062051040
```

9.4 friend

The **friend** command refers to context friend, which contains commands to add friendly APs. The **friend** command is accessible from the **mitigator** context of the CLI.

9.4.1 frlist

Use the **frlist** command to add a Wireless AP to the list of friendly APs. Use the **no** form of the command to delete a Wireless AP from the list of friendly APs.

Syntax

```
frlist <mac> [ssid <string>] [channel <value>] [desc <string>]
no frlist <mac> [ssid <string>] [channel <value>] [desc <string>]
```

Parameters

mac	Specifies Wireless AP's MAC address
ssid <string>	Specifies Wireless AP's SSID
channel <value>	Specifies Wireless AP's current operating channel
desc <string>	Specifies Wireless AP's brief description

Examples

The following example adds a Wireless AP to the list of friendly APs.

```
EWC.enterasys.com:mitigator:friend# frlist 00:0E:8C:1E:A0:10 ssid CNL201-brg-AP-wifi channel 1 desc friendly_ap
```

Note: After you have added a Wireless AP to the list of friendly APs, you must run the **apply** command to implement the changes.

10

mobility Commands

Multiple Enterasys Wireless Controllers on a network can share and exchange client session information, which enables a wireless device to roam between Wireless APs on different Enterasys Wireless Controllers without service interruption.

This section describes the commands required to configure the Mobility options for the Enterasys Wireless Controller. These commands are located in the **mobility** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **mobility** context:

- mrole
- mport
- mheartbeat
- slpreg
- agent
- secmode
- mdismethod
- mmanagerip

10.1 mrole

Use the **mrole** command to set the role of the Enterasys Wireless Controller.

Syntax

```
mrole (none|manager|agent)
```

Parameters

none	Removes role designations from the controller
manager	Sets the role of the Enterasys Wireless Controller to Manager
agent	Sets the role of the Enterasys Wireless Controller to Agent

Examples

The following example sets the role of the Enterasys Wireless Controller as a Mobility Agent.

```
EWC.enterasys.com:mobility# mrole agent
```

10.2 mport

Use the **mport** command to select the port to be used by the **Mobility** feature.

Syntax

```
mport <esaX>
```

Parameters

<esaX>	Specifies the ESA port, where X refers to the port number

Examples

The following example selects the esa3 port

```
EWC.enterasys.com:mobility# mport esa3
```

10.3 mheartbeat

The Enterasys Wireless Controller that has the VNManager designation sends regular Heartbeat messages containing information regarding wireless device session changes to the VNAgents, and waits for an update message to come back.

Use the **mheartbeat** command to set the time interval (in seconds) for the connection establishment response between the Mobility Agent and the Mobility Manager.

Syntax

```
mheartbeat <value>
```

Parameters

<value>	Specifies the interval time in seconds between outgoing heartbeats

Examples

The following example sets the outgoing heartbeats to occur at 5 second intervals.

```
EWC.enterasys.com:mobility# mheartbeat 5
```

10.4 slpreg

Use the **slpreg** command to enable SLP registration. Use the **no** form of the command to disable it.

Syntax

```
slpreg
no slpreg
```

Parameters

None

Examples

The following example enables SLP registration

```
EWC.enterasys.com:mobility# splreg
```

10.5 agent

Use the **agent** command to add, remove, or approve an agent on the network by its IP address.

Note: The role of the Enterasys Wireless Controller must be set to Manager before this option becomes available. For more information, see “mrole” on page 10-1.

Syntax

```
agent (add|remove|approve) <IP Address>
```

Parameters

add	Adds an agent to the network
remove	Removes an agent from the network
approve	Approves an agent on the network
<IP Address>	Specifies the IP address of the agent

Examples

The following example adds an agent to the network

```
EWC.enterasys.com:mobility# agent add 10.0.0.1
```

The following example removes an agent from the network

```
EWC.enterasys.com:mobility# agent remove 10.0.2.4
```

The following example approves an agent on the network

```
EWC.enterasys.com:mobility# agent approve 10.0.0.1
```

10.6 secmode

Use the **secmode** command to set the Security Mode to allow only approved Agents to connect to the manager, or allow all agents to connect.

Syntax

```
secmode (approved|none)
```

Parameters

approved	Allows only approved agents to connect to the manager
none	Allows all agents are to connect to the manager

Examples

The following example configures the security mode to have no restrictions, allowing all agents to connect to the manager

```
EWC.enterasys.com:mobility# secmode none
```

10.7 mdismethod

Use the **mdismethod** command to locate the Mobility Manager on the network.

Syntax

```
mdismethod (slpd|static)
```

Parameters

slpd	Uses the Service Location Protocol (SLP) Discovery method
static	Uses a statically configured IP address for detection

Examples

The following example uses the SLP discovery method

```
EWC.enterasys.com:mobility# mdismethod slpd
```

10.8 mmanagerip

Use the **mmanagerip** to specify the IP address of the Mobility Manager.

Note: The role of the Enterasys Wireless Controller must be set to Agent before this option becomes available. For more information, see “mrole” on page 10-1.

Syntax

```
mmanagerip <IP Address>
```

Parameters

<IP Address>	Specifies the IP address of the VN Manager

Examples

The following example changes the IP address of the Mobility Manager.

```
EWC.enterasys.com:mobility# mmanagerip 195.160.1.39
```

11

schedule_backup Commands

This section describes commands for scheduling the backup of the following reports and database:

- Software configurations
- CDRs
- Logs
- Audit Report
- Rogue APs Report

This section describes commands which manage scheduling options for the backup of data to an FTP or SCP address. These commands are located in the **schedule_backup** context of the CLI.

Note: If you do not specify the FTP or SCP server's IP address, the reports and database will be saved on the local drive of the HiPath Wireless Controller.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **schedule_backup** context:

- dir
- freq
- password
- protocol
- server
- starttime
- type
- user

Note: After running the **schedule_backup** commands, you must run the **apply** command to implement the changes.

11.1 dir

Use the **dir** command to specify a directory to contain backup data on the FTP or SCP server.

Syntax

```
dir <path>
```

Parameters

<path>	Specifies the directory path

Examples

The following example specifies the directory path for backup data.

```
EWC.enterasys.com:schedule_backup# dir /home/user/destdir
```

11.2 freq

Use the **freq** command to specify the frequency of software backups.

Syntax

```
freq (daily everyday|weekday)|(weekly 0,1,2,3,4,5,6)|(monthly <date>)|never
```

Parameters

daily	Indicates that backups will occur on a daily basis
everyday	Configures backup to occur every day of the week
weekday	Configures backup to occur from Monday to Friday only
weekly	Indicates that backups will occur on weekly basis
0	Configures backup scheduling to include Sunday
1	Configures backup scheduling to include Monday
2	Configures backup scheduling to include Tuesday
3	Configures backup scheduling to include Wednesday
4	Configures backup scheduling to include Thursday
5	Configures backup scheduling to include Friday
6	Configures backup scheduling to include Saturday
monthly	Indicates that backups will occur on a monthly basis
<date>	Specifies a calendar day
never	Indicates that backups will not occur

Examples

The following example sets the software backups to occur from Monday to Friday

```
EWC.enterasys.com:schedule_backup# freq daily weekday
```

The following example sets the software backups to occur every Tuesday and Thursday

```
EWC.enterasys.com:schedule_backup# freq weekly 2,4
```

The following example sets the software backups to occur on the 15th day of every month

```
EWC.enterasys.com:schedule_backup# freq monthly 15
```

The following example disables all backup scheduling

```
EWC.enterasys.com:schedule_backup# freq never
```

11.3 password

Use the **password** command to specify the password of the user name on the FTP or SCP server.

Note: The user name must be specified using the **user** command. For more information, see "user" on page 11-5.

Syntax

```
password <string>
```

Parameters

<string>	Specifies a password for a user on the FTP or SCP server

Examples

The following command specifies a password for the user on the server.

```
EWC.enterasys.com:schedule_backup# password rYm239sJ
```

11.4 protocol

Use the **protocol** command to specify the appropriate protocol to use when communicating with the destination server.

Syntax

```
protocol [ftp|scp]
```

Parameters

ftp	Specifies the FTP protocol
scp	Specifies the SCP protocol

Examples

The following example sets the protocol to SCP.

```
EWC.enterasys.com:schedule_backup# protocol scp
```

11.5 server

Use the **server** command to specify the IP address of the destination server for backup data.

Syntax

```
server <IP Address>
```

Parameters

<IP Address>	Specifies the IP address of the FTP or SCP server

Examples

The following example sets the IP address of the server receiving backup data.

```
EWC.enterasys.com:schedule_backup# server 192.168.1.17
```

11.6 starttime

Use the **starttime** command to specify the time of day to start a scheduled backup.

Note: The scheduled task time must be set to daily, weekly, or monthly before the start time can be specified. For more information, see “freq” on page 11-2.

Syntax

```
starttime <HH>:<mm>
```

Parameters

<HH>	Specifies the hour (in a 24 hour clock format) to start a scheduled backup
<mm>	Specifies the minute to start scheduled backup

Examples

The following example sets the start time of a scheduled backup to 1:16 PM

```
EWC.enterasys.com:schedule_backup# starttime 13:16
```

11.7 type

Use the **type** command to indicate the data types to backup.

Syntax

```
type (configuration|cdrs|all|logs|audit|rogue)
```

Parameters

configuration	Indicates that configuration files will be backed up
cdrs	Indicates that call detail records will be backed up

all	Indicates that all configuration, call detail records, log files, audit files, and rogue files will be backed up
logs	Indicates that log files will be backed up
audit	Indicates that audit files will be backed up
rogue	Indicates that rogue files will be backed up

Examples

The following example indicates that audit files are to be backed up

```
EWC.enterasys.com:schedule_backup# type audit
```

11.8 user

Use the **user** command to specify the user name of an account on the FTP or SCP server.

Syntax

```
user <id>
```

Parameters

<id>	Specifies a user name

Examples

The following example specifies a username for the server.

```
EWC.enterasys.com:schedule_backup# user admin
```

12

schedule_upgrade Commands

Use the **schedule_upgrade** context to access the commands for scheduling an upgrade and back up of the controller's software. The **schedule_upgrade** context is accessible from the root context of the CLI.

Note: schedule_upgrade is not the command. It is the context. You must be in the **schedule_upgrade** context to access the commands for scheduling the upgrade and backup of the controller's software. The commands for scheduling the upgrade and back up of the controller's image is provided in the following sections.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **schedule_upgrade** context:

- schld_upgrd
- upgrade_backup

12.1 schld_upgrd

Use the **schld_upgrd** command to schedule a local or remote upgrade of the Enterasys Wireless Controller's software. Use the **no** form of the command to delete the scheduled upgrade.

This command is accessible from the **schedule_upgrade** context.

Syntax

```
[no] schld_upgrd <MM:DD:hh:mm> (local <image_name>) |(remote <server> <user>
<password> <dir> <image_name>)
```

Parameters

MM	Month on which the upgrade will be carried out
DD	The date on which the upgrade will be carried out
hh:mm	The time (in 24-hour format) at which the upgrade will be carried out
local	Specifies that the new software will be downloaded locally from the Enterasys Wireless Controller
image name	The new software's file name
remote	Specifies that the new software will be downloaded from the remote FTP server
server	The remote FTP server where the image file is located

user	The user name to access the FTP server
password	The password to access the FTP server
dir	The path to the directory where the new software is stored on the FTP server
image name	The new software's file name

Examples

The following example schedules a local upgrade.

```
EWC.enterasys.com:schedule_upgrade# schld_upgrd 06:01:12:00 local AC-MV-
07.41.03.0003-1.gps
```

Note: Before you can schedule a local uprade, you must download the upgrade image to the controller.

Note: If you want to delete the existing local upgrade schedule, you must add **no** before the local upgrade syntax as shown in the following example.
EWC.enterasys.com:schedule_upgrade# **no schld_upgrd**

The following example schedules a remote upgrade.

```
EWC.enterasys.com:schedule_upgrade# schld_upgrd 06:01:12:00 remote 192.168.4.10
test abc123 /ac/rpm/build07.41.03.0003 AC-MV-07.41.03.0003-1.gps
```

Note: If you want to delete the existing remote upgrade schedule, you must add **no** before the remote upgrade syntax as shown in the following example.
EWC.enterasys.com: schedule_upgrade# **no schld_upgrd**

12.2 upgrade_backup

Use the **upgrade_backup** command to create a rescue backup of the existing software of the Enterasys Wireless Controller on the remote FTP server. Use the **no** form of the command to delete the remote rescue backup.

The **upgrade_backup** command is accessible from the **schedule_upgrade** context.

Syntax

```
upgrade_backup (local|flash|remote <server> <user> <password> <dir> <file>)
no upgrade_backup
```

Parameters

upgrade_backup	Specifies to backup the existing software of the Enterasys Wireless Controller before initiating the upgrade process
flash <filename>	Specifies that the backup image of the existing software of the Enterasys Wireless Controller is to be saved on the flash card. This option is only available if an external flash card has been mounted on the controller. Backup file name can optionally be provided, but it must end with "-rescue-user.tgz".

local	Specifies that the backup image of the existing software of the Enterasys Wireless Controller is to be saved locally. Option is not available on C2400.
remote	Specifies that the backup image of the existing software of the Enterasys Wireless Controller is to be created on the remote FTP server
server	The FTP server where the backup image will be created
user	The user name to access the FTP server
password	The password to access the FTP server
dir	The directory where the backup image will be created on the FTP server
file	The file name that you want to assign to the backup image. Filename must end with ".tgz".

Examples

In the following example, the backup image is created on the ftp server.

```
EWC.enterasys.com:schedule_upgrade# upgrade_backup remote 192.168.4.181 admin abc123/ myDir/ backup.tgz
```

In the following example, the backup image is created on the external flash.

```
EWC.enterasys.com:schedule_upgrade# upgrade_backup flash backupToFlash-rescue-user.tgz
```

The following example deletes the upgrade backup.

```
EWC.enterasys.com:schedule_upgrade# no upgrade_backup
```

13

snmp Commands

The Enterasys Wireless Controller supports the Simple Network Management Protocol (SNMP) for retrieving statistics and configuration information.

This section describes commands which manage SNMP settings for the Enterasys Wireless Controller. These commands are located in the **snmp** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **snmp** context:

- contact
- context
- enable
- engine-id
- location
- severity
- trap-manager-v1v2
- trap-manager-v3
- user
- show
- rwcommunity
- port
- publish-ap
- show

13.1 contact

Use the **contact** command to identify the name of the SNMP administrator.

Syntax

```
contact <string>
```

Parameters

<string>	Specifies the name of the person enabling SNMP traps on the system

Examples

The following example specifies a name to identify the SNMP administrator.

```
EWC.enterasys.com:snmp# contact Bill
```

13.2 context

Use the **context** command to add an SNMPv3 context.

Syntax

```
context <string>
```

Parameters

<string>	Specifies the context name

Examples

The following example specifies the SNMPv3 context.

```
EWC.enterasys.com:snmp# context context1
```

13.3 enable

Use the **enable** command to enable and configure SNMP.

Syntax

```
enable (none|v1v2|v3) [<contact> <location> <rcommunity> <rwcommunity>
(1|2|3|4|5) <1-65535>]
```

Parameters

none	Disables SNMP
(v1v2|v3)	Enables either SNMPv1/V2 or SNMPv3
<contact>	Specifies the name of the SNMP administrator
<location>	Specifies a description for the location of the SNMP administration machine
<rcommunity>	Specifies a name for the read-only network management community
<rwcommunity>	Specifies a name for the read-write network management community
1	Forwards the SNMP trap with the Critical severity level
2	Forwards the SNMP trap with the Major severity level
3	Forwards the SNMP trap with the Minor severity level
4	Forwards the SNMP trap with the Informational severity level
5	Forwards the SNMP trap with the Trace severity level
<0-65555>	Specifies the destination port for the SNMP traps

Examples

The following example enables SNMPv3.

```
EWC.enterasys.com:snmp# enable v3
```

13.4 engine-id

Use the **engine-id** command to configure the SNMPv3 engine ID for the Enterasys Wireless Controller running the SNMP agent.

Syntax

```
engine-id <string> [auto-gen]
```

Parameters

<string>	Specifies the SNMPv3 engine ID for the Enterasys Wireless Controller running the SNMP agent. The string must be from 5 to 32 characters in length when auto-gen is not selected, and from 1 to 27 characters when auto-gen is selected.
[auto-gen]	Automatically generates the SNMPv3 engine ID from the manually entered string.

Examples

The following example specifies the SNMPv3 engine ID of the SNMP agent. Note that resetting the engine-id will reset all users.

```
EWC.enterasys.com:snmp# engine-id aaaaaaa
All users will be reset.
(yes/no):no
Warning : Operation to update engine ID cancelled.
```

13.5 location

Use the **location** command to enter a descriptive string indicating the physical location of the Enterasys Wireless Controller running the SNMP agent.

Syntax

```
location <string>
```

Parameters

<string>	Specifies the location Enterasys Wireless Controller running the SNMP agent

Examples

The following example specifies the location of the SNMP agent.

```
EWC.enterasys.com:snmp# location Blue Office - Second Floor
```

13.6 port

Use the **port** command to specify the destination port for the SNMP traps.

Syntax

```
port <value>
```

Parameters

<value>	Specifies the trap port of the SNMP manager. The value can range from 1 to 65535.

Examples

The following example sets the trap port of the SNMP manager to 163.

```
EWC.enterasys.com:snmp# port 163
```

13.7 publish-ap

Use the **publish-ap** command to enable or disable SNMP publishing of the access point as an interface to the Enterasys Wireless Controller.

Syntax

```
publish-ap (enable|disable)
```

Parameters

enable | disable	Enables or disables publishing of the access point as an interface to the controller.

Examples

The following example enables SNMP publishing.

```
EWC.enterasys.com:snmp# publish-ap enable
```

If you attempt to enable SNMP publish when LLDP is enabled on one or more APs, you will get the following warning:

```
WARNING: LLDP is enabled for some Wireless APs. Would you like to continue?
(C) Cancel
(P) Proceed
(O) Disable LLDP and proceed
```

Type one of the following:

- **C** – Cancels the SNMP configuration and returns to the AP context.
- **P** – Enables SNMP publishing and maintains LLDP enabled
- **O** – Enables SNMP and disables LLDP

13.8 rcommunity

Use the **rcommunity** command to set the name of the read-only community.

Syntax

```
rcommunity <string>
```

Parameters

<string>	Specifies the name used for the read-only community

Examples

The following example sets the name of the read-only community.

```
EWC.enterasys.com:snmp# rcommunity public
```

13.9 rwcommunity

Use the **rwcommunity** command to specify the name of the read-write community. This community allows the modification of stored data on the administrative system.

Syntax

```
rwcommunity <string>
```

Parameters

<string>	Specifies the name used for the read-write community

Examples

The following example sets the name of the read-write community.

```
EWC.enterasys.com:snmp# rwcommunity private
```

13.10 severity

Use the **severity** command to configure the Enterasys Wireless Controller to send SNMP traps of the specified severity level.

Syntax

```
severity (1|2|3|4|5)
```

Parameters

1	Forwards the SNMP trap with the Critical severity level
2	Forwards the SNMP trap with the Major severity level
3	Forwards the SNMP trap with the Minor severity level
4	Forwards the SNMP trap with the Informational severity level
5	Forwards the SNMP trap with the Trace severity level

Examples

The following example forwards traps having the Critical level of severity.

```
EWC.enterasys.com:snmp# severity 2
```

13.11 show

Use the **show** command in the SNMP context to display all SNMP configuration information or just information about configured SNMPv3 users.

Syntax

```
show [user]
```

Parameters

user	Display only configured users.

Examples

The following example lists only the SNMPv3 users, when in the SNMP context.

```
EWC.enterasys.com:snmp# show user
User    Authentication   ProtocolAuth   ProtocolPriv   Enabled
test1   noauthnopriv     none           none           False
```

Refer to “user” on page 13-7 for descriptions of the values in the various columns of this output.

13.12 trap-manager-v1v2

Use the **trap-manager-v1v2** command to identify either the primary or secondary machine monitoring SNMPv1/v2 traps by IP address.

Syntax

```
trap-manager-v1v2 <1-2> (<IP Address>| delete)
```

Parameters

<1-2>	Identifies the primary or secondary machine monitoring SNMPv1/v2 traps
<IP Address>	Specifies the IP address of the machine monitoring SNMPv1/v2 traps
delete	Delete the specified trap manager.

Examples

The following example specifies the IP address of the primary machine monitoring SNMPv1/v2 traps.

```
EWC.enterasys.com:snmp# trap-manager-v1v2 1 192.168.1.5
```

The following example deletes the secondary machine monitoring SNMPv1/v2 traps.

```
EWC.enterasys.com:snmp# trap-manager-v1v2 2 delete
```

13.13 trap-manager-v3

Use the **trap-manager-v3** command to identify either the primary or secondary machine monitoring SNMPv3 traps by IP address.

Syntax

```
trap-manager-v3 (1|2) (A.B.C.D user <username> | delete)
```

Parameters

<1-2>	Identifies the primary or secondary machine monitoring SNMPv3 traps
<A.B.C.D>	Specifies the IP address of the machine monitoring SNMPv3 traps
user <username>	Specifies the SNMPv3 user to configure for use with SNMPv3 traps

Examples

The following example specifies the IP address of the primary machine monitoring SNMPv3 traps and the SNMPv3 user "admin."

```
EWC.enterasys.com:snmp# trap-manager-v3 1 192.168.1.5 user admin
```

The following example deletes the primary trap manager configured in the previous example.

```
EWC.enterasys.com:snmp# trap-manager-v3 1 delete
```

13.14 user

Use the **user** command to configure SNMP v3 users and security.

Syntax

```
user <username> security (noAuthNoPriv | authNoPriv (md5|sha) <authpassword> |
authPriv (md5|sha) <authpassword> des <privpassword>)
user <username> disable|enable
user <username> delete
```

Parameters

<username>	Specifies the SNMPv3 user to configure for use with SNMPv3 traps
security (noAuthNoPriv | authNoPriv | authPriv)	Specifies the security options to use with this SNMPv3 user (Noauthnopriv, Authnopriv, or Authpriv)
md5 | sha	Specifies the authentication protocol to use when security level is set to authNoPriv or authPriv.
<authpassword> des	Specifies the authentication password and the DES protocol to use when security level is set to authNoPriv or authPriv. DES must be used when the security level is set to authPriv.
<privpassword>	Specifies the privacy password to use when security level is set to authPriv.
enable | disable	Enables or disables an existing user
delete	Deletes an existing user

Examples

The following example creates an SNMPv3 user named “test” with an authPriv security level using MD5, an authentication password of “tester1234” and a privacy password of “tester1234.”

```
EWC.enterasys.com:snmp# user test security authPriv md5 tester1234 des test1234
```

14

syslog Commands

This section describes commands to configure System Log settings on the Enterasys Wireless Controller. These commands are located in the **syslog** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **syslog** context:

- audmsg
- facility
- svcmsg
- syslogip

14.1 audmsg

Use the **audmsg** command to enable service messages. Use the **no** form of the command to disable them.

Syntax

```
audmsg
no audmsg
```

Parameters

None

Examples

The following example enables service messages on the Enterasys Wireless Controller

```
EWC.enterasys.com:syslog# audmsg
```

14.2 facility

Use the **facility** command to update application and service logs to the syslog server.

Note: Application logs and service logs cannot use the same log level at the same time.

Syntax

```
facility (application|service|audit) (0|1|3|4|5|6)
```

Parameters

application	Indicates that application logs are to be updated
service	Indicates that service logs are to be updated
audit	Indicates that audit logs are to be updated
0	Sends the log with the Emergency severity level to the syslog server
1	Sends the log with the Alert severity level to the syslog server
3	Sends the log with the Error severity level to the syslog server
4	Sends the log with the Warning severity level to the syslog server
5	Sends the log with the Notice severity level to the syslog server
6	Sends the log with the Info severity level to the syslog server

Examples

The following example selects the application log level 3 to be sent to the syslog server

```
EWC.enterasys.com:syslog# facility application 3
Successfully updated application logs to 3.
```

14.3 svcmsg

Use the **svcmsg** command to enable DHCP and startup management task messages. Use the **no** form of the command to disable these and use log and traces messages only.

Syntax

```
svcmsg
no svcmsg
```

Parameters

None

Examples

The following example enables service messages on the system

```
EWC.enterasys.com:syslog# svcmsg
Successfully turned on service messages.
```

The following example disables service messages

```
EWC.enterasys.com:syslog# no svcmsg
Successfully turned off service messages.
```

14.4 syslogip

Use the **syslogip** command to configure up to three syslog servers. Use the **no** form of the command to delete a server.

Note: Use **show syslog** to display system log levels. For more information, see “show syslog” on page 3-55.

Syntax

```
syslogip <#> <IP Address> [enable|disable]
no syslogip
```

Parameters

<#>	Specifies the index number of the system log ID
<IP Address>	Specifies the IP address to be configured
enable	Enables the server
disable	Disables the server

Examples

The following example specifies the IP address of a syslog server and enables it

```
EWC.enterasys.com:syslog# syslogip 1 143.23.34.52 enable
Successfully updated syslogip 1.
```

The following example deletes the syslog server

```
EWC.enterasys.com:syslog# no syslogip 1
Successfully removed syslogip 1.
```

15

time Commands

Network elements on the Enterasys Wireless Controller can be synchronized to a universal clock in one of two ways:

- using the Enterasys Wireless Controller's own system time
- using the Network Time Protocol

The commands described in this section are used to select and configure these options, and are located in the **time** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

Note: After you run the following **time** commands, you must run the **apply** command to implement the changes.

The following commands are available in the **time** context:

- clock
- date
- ntp
- ntpip
- tz

15.1 clock

Use the **clock** command to set the system time.

The Network Time Protocol must be disabled before this command can be used. For more information, see "ntp" on page 15-2.

Syntax

```
clock <hh:mm>
```

Parameters

hh	Specifies the current hour (in 24 hour clock format)
mm	Specifies the current minute

Examples

The following example sets the system time to 12:01pm

```
EWC.enterasys.com:time# clock 12:01
```

Note: After you run the **clock** command, you must run the apply command to implement the changes.

15.2 date

Use the **date** command to set the system date.

Note: The Network Time Protocol must be disabled before this command can be used. For more information, see “ntp” on page 15-2.

Syntax

```
date dd:mm:yyyy
```

Parameters

dd	Specifies the day
mm	Specifies the month
yyyy	Specifies the year

Examples

The following example sets the date to January 17, 2099

```
EWC.enterasys.com:time# date 17:01:2099
```

15.3 ntp

Use the **ntp** command to use the Network Time Protocol (NTP). Use the **no** form of the command to disable it.

Syntax

```
ntp [2|3]
(no) ntp [1|2|3]
```

Parameters

2	Specifies to use the external NTP Server to synchronize the network time
3	Specifies to use the internal NTP Server to synchronize the network time

Examples

The following example specifies to use the internal NTP Server to synchronize the network time

```
EWC.enterasys.com:time# ntp 3
```

Note: If you want to use the external NTP Server, you must configure the NTP Server's IP address by running the **ntpip** command. For more information, see the following section.

15.4 ntpip

Use the **ntpip** command to configure the IP address of up to 3 standard NTP time servers. Use the **no** form of the command to remove an IP address by its index number.

Syntax

```
ntpip (1|2|3) <IP Address>
no ntpip (1|2|3)
```

Parameters

1|2|3	Indicates the index number on the list of configured NTP time servers
<IP Address>	Specifies the IP address of an NTP time server

Examples

The following example configures the IP address of an NTP time server and assigns it an index value of 2

```
EWC.enterasys.com:time# ntpip 2 192.168.4.89
```

15.5 tz

Use the **tz** command to set time zone information for the Enterasys Wireless Controller.

Syntax

```
tz continent <continent> country <country> region <region>
```

Parameters

<continent>	Specifies the continent
<country>	Specifies the country
<region>	Specifies the region

Examples

The following example sets the time zone information

```
EWC.enterasys.com:time# tz continent america country united states region new_york
```

Note: The Enterasys Wireless Controller reboots when the time zone is changed.

16

traffic_capture Commands

The **traffic_capture** command refers to **traffic_capture** context, which contains the commands to manage the TCPDump. The **traffic_capture** is accessible from the root context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **traffic_capture** context:

- file_name
- size
- destination
- interface
- delete
- list
- start
- stop
- show
- show interfaces

16.1 file_name

Use the **file_name** command to specify a file name for the TCPDump. The **file_name** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
file_name <fileName>
```

Parameters

<fileName>	Specifies the file name for the TCPDump

Examples

The following example specifies the file name as TrafficCapture for the TCPDump.

```
EWC.enterasys.com:traffic_capture# file_name TrafficCapture
```

Note: If you do not assign any file name to the TCPDump, the CLI gives a default name *mgmt_traffic_dump.cap*. The CLI enforces *.cap* file extension to the TCPDump file.

16.2 size

Use the **size** command to specify the file size of TCPDump file. The **size** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
size <filesize>
```

Parameters

<filesize>	Specifies the file size of TCPDump file

Examples

The following example specifies the file size of the TCPDump file as 5Mb.

```
EWC.enterasys.com:traffic_capture# size 5
```

Note: TCPDump has file size limitations. The limitations are based on the following factors:
• Platform Type — whether TCP Dump is stored on the local drive of C20, C100/C1000 or C2400 controllers.
• Storage destination — whether TCPDump is stored on the local drive or the CF card.
The following matrix provides the size limitations for various types of platforms and the two storage destinations — CF card and the controller's local drive.

If you try to save the TCPDump file that is bigger in size than what is described in the above matrix, the CLI will return the following message: **File size is bigger than the available space.**

16.3 destination

Use the **destination** command to specify the destination — Compact Flash (CF) card or local drive — for the TCPDump file to be stored. The **destination** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
destination <(flash|local)>
```

Parameters

<flash>	Specifies the TCPDump file to be stored on CF card
<local>	Specifies the TCPDump file to be stored on local

Examples

The following example specifies the TCPDump file to be stored on CF card.

```
EWC.enterasys.com:traffic_capture# destination flash
```

Note: The destination command is accessible only in the Enterasys Wireless C2400 Controller and only when the CF card is enabled.

16.4 interface

Use the **interface** command to specify the interface on which the exception traffic is to be captured.

Note: You can choose any of the following interfaces:
- Management Port (eth0)
- Physical esa ports
- Defined VNS

Syntax

```
interface <interfacename>
```

Parameters

<interfacename>	The interface name on which the exception traffic is to be captured

Parameters

None

Examples

The following example specifies the exception traffic to be captured on esa0.

```
EWC.enterasys.com:traffic_capture# interface esa0
```

16.5 delete

Use the **delete** command to delete the TCPDump file. The **delete** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
delete <# from the capture file list>
```

Parameters

<# from the capture file list>	The sequence in which the files are listed in the capture file list

Examples

The following example specifies the file # 1 in the "TCPDump file capture" list to be deleted.

```
EWC.enterasys.com:traffic_capture# delete 1
```

Note: To display the "TCPDump file capture" list, you must run the **list** command from the **traffic_capture** context of the CLI. For more information, see the following section.

16.6 list

Use the **list** command to display the "TCPDump file capture" list. The **list** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
list
```

Parameters

None

Examples

The following example displays the list of TCPDump file capture.

```
EWC.enterasys.com:traffic_capture# list
Traffic Capture Files:
    1:mgmt_traffic_dump.cap
    2:mgmt_traffic_dump.cap (flash)
    3:mgmt_traffic_dump-01.cap (flash)
    4:mgmt_traffic_dump-02.cap (flash)
    5:dhcp-relay-01.cap (flash)
    6:third-party-01.cap (flash)
    7:mgmt_traffic_dump-03.cap (flash)
```

Note: The files that are stored on the CF card have flash suffixed to their file names. For example, `mgmt_traffic_dump.cap (flash).`
The files that are stored on the local drive of the controller do not have anything suffixed to them.

Note: You can save only one TCPDump file on the local drive.

16.7 start

Use the **start** command to start capturing the exception traffic to and from the management plane. The capture includes the following:

- All traffic on the management port (eth0)
- Exception traffic for the physical esa ports and defined VNS

The **start** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
start
```

Parameters

None

Examples

The following example specifies to start capturing the exception traffic.

```
EWC.enterasys.com:traffic_capture# start
```

16.8 stop

Use the **stop** command to stop capturing the exception traffic to and from the management plane. The **stop** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
stop
```

Parameters

None

Examples

The following example specifies to stop capturing the exception traffic.

```
EWC.enterasys.com:traffic_capture# stop
```

16.9 show

Use the **show** command to display the configuration for capturing the exception traffic to and from the management plane.The **show** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
show
```

Parameters

None

Examples

The following example displays the configuration for capturing the exception traffic to and from the management plane.

```
EWC.enterasys.com:traffic_capture# show
Interface: esa2
Size: 30(MB).
Filename: mgmt_traffic_dump.cap
Destination: local
Capture Status: stopped
Traffic Capture Files:
    1:mgmt_traffic_dump.cap
```

16.10 show interfaces

Use the **show interfaces** command to display the physical and virtual ports for which the exception traffic can be captured.The **show interfaces** command is accessible from the **traffic_capture** context of the CLI.

Syntax

```
show interfaces
```

Parameters

None

Examples

The following example displays the physical and virtual ports for which the exception traffic can be captured.

```
EWC.enterasys.com:traffic_capture# show interfaces
eth0
esa0
esa1
esa2
esa3
CNL-208-202brAC
CNL-209-AAA
CNL-209-AAADyn
CNL-209-bri
CNL-209-briAC
CNL-209-briAC_AAA
```

17

users Commands

This section describes commands used to create and manage user accounts on the network. These commands are found within the **users** context of the CLI.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **users** context:

- id
- pwd

17.1 id

Use the **id** command to create user or administrator accounts on the system. In conjunction with the **id** command, you must specify and confirm a password for the account. The password must be 8–24 alphanumeric characters long.

Syntax

```
id <userid> <admin|guestportal|readonly>
```

Parameters

userid	Specifies a name for the account
admin	Sets account type to administrator
guestportal	Sets account type to guestportal administrator
readonly	Sets account type to readonly

Examples

The following example creates the read-only user account “abby” on the system

```
EWC.enterasys.com:users# id abby readonly
Please input password:
Please confirm password:
Successfully created user abby.
```

The following example creates the administrator account “fred” on the system

```
EWC.enterasys.com:users# id fred admin
```

```
Please input password:
Please confirm password:
Successfully created user fred.
```

The following example creates a guest administrator user account called “tester” on the system

```
EWC.enterasys.com:users# id tester guestportal
Please input password:
Please confirm password:
Successfully created user tester.
```

Note: A guest administrator user created using the guestportal user type can only login to the system using the GUI.

17.2 pwd

Use the **pwd** command to change the password for a specified account. The password must be 8–24 alphanumeric characters long.

Syntax

```
pwd <userid>
```

Parameters

<userid>	Specifies the name of the account

Examples

The following example changes the password for the account named “fred”

```
EWC.enterasys.com:users# pwd fred
Please input new password:
Please confirm new password:
```

18

VNS Commands (vnsmode)

This section describes commands used to define and configure Virtual Network Services (VNS) for the network. These commands are located in the **vnsmode** context of the CLI. Execute the **vnsmode** command at the root level to enter vnsmode context.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **vnsmode** context:

- adminctr — See adminctr for commands in the **vnsmode:adminctr** context.
- create
- das — See das for commands in the **vnsmode:das** context.
- default-policy — See default-policy for commands in the **vnsmode:default-policy** context.
- delete
- radius — See radius for commands in the **vnsmode:radius** context.
- rateprofile — See rateprofile for commands in the **vnsmode:rateprofile** context.
- <named-VNS> — See <named-VNS> for commands in the **vnsmode:<named-VNS>** context.

18.1 adminctr

Executing the **adminctr** command moves you into the **vnsmode:adminctr** context in which you configure several global QoS (Quality of Service) settings. This context contains global admission control commands to configure flexible client access and to control the amount of bandwidth for voice and video applications on Wireless APs.

The following commands are available in the **vnsmode:adminctr** context:

- flex-client-access
- max-video-assoc
- max-video-reassoc
- max-voice-assoc
- max-voice-reassoc

18.1.1 flex-client-access

Use the **flex-client-access** command to configure flexible client access (FCA) to the wireless medium. FCA can be adjusted in multiple steps between packet fairness and airtime fairness using this command. This command is available in the vnsmode:adminctr context.

Syntax

```
flex-client-access 100%-packet | mostly-packet | mixed | mostly-airtime | 100%-airtime
```

Parameters

100%-packet	Specifies 100% packet access to the wireless medium
mostly-packet	Specifies mostly packet access to the wireless medium
mixed	Specifies mixed access to the wireless medium
mostly-airtime	Specifies mostly airtime access to the wireless medium
100%-airtime	Specifies 100% airtime access to the wireless medium

Examples

The following example sets the FCA to 100% packet access.

```
EWC.enterasys.com:vnsmode:adminctr# flex-client-access 100%-packet
```

18.1.2 max-video-assoc

Use the **max-video-assoc** command to configure the maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new video stream.

Syntax

```
max-video-assoc <0-100>
```

Parameters

<0-100>	Specifies the maximum allowable bandwidth as a percentage of total bandwidth.

Examples

The following example sets the maximum video bandwidth for new streams to 40% of total bandwidth.

```
EWC.enterasys.com:vnsmode:adminctr# max-video-assoc 40
```

Note: After you run the **max-video-assoc** command, you must run the **apply** command to implement the changes.

18.1.3 max-video-reassoc

Use the **max-video-reassoc** command to set the maximum allowed overall bandwidth on the new AP when a client with an active video stream roams to a new AP and requests admission for the video stream.

Syntax

```
max-video-reassoc <0-100>
```

Parameters

<0-100>	Specifies the maximum allowable bandwidth as a percentage of total bandwidth.

Examples

The following example sets the maximum video bandwidth for roaming streams to 60% of total bandwidth.

```
EWC.enterasys.com:vnsmode:adminctr# max-video-reassoc 60
```

Note: After you run the **max-video-reassoc** command, you must run the **apply** command to implement the changes.

18.1.4 max-voice-assoc

Use the **max_voice_assoc** command to set the maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new voice stream.

Syntax

```
max-voice-assoc <0-100>
```

Parameters

<0-100>	Specifies the maximum allowable bandwidth as a percentage of total bandwidth.

Examples

The following example sets the maximum voice bandwidth for new streams to 60% of total bandwidth.

```
EWC.enterasys.com:vnsmode:adminctr# max-voice-assoc 60
```

Note: After you run the **max-voice-assoc** command, you must run the **apply** command to implement the changes.

18.1.5 max-voice-reassoc

Use the **max-voice-reassoc** command to set the maximum allowed overall bandwidth on the new AP when a client with an active voice stream roams to a new AP and requests admission for the voice stream.

Syntax

```
max-voice-reassoc <0-100>
```

Parameters

<0-100>	Specifies the maximum allowable bandwidth as a percentage of total bandwidth.

Examples

The following example sets the maximum voice bandwidth for roaming streams to 80%

```
EWC.enterasys.com:vnsmode:adminctr# max-voice-reassoc 80
```

Note: After you run the **max-voice-reassoc** command, you must run the **apply** command to implement the changes.

18.2 create

Use the **create** command to create a new VNS. This command is available in the **vnsmode** context. After you create a VNS with this command, you can configure additional parameters in the **vnsmode:<named-VNS>** context. Refer to "<named-VNS>" on page 18-34 for more information.

Syntax

```
create <vns name> wlans <WLANS name> pol <policy name>
```

Parameters

<vns name>	Specifies a name for this VNS
wlans <WLANS name>	Specifies a WLAN Service for this VNS
pol <policy name>	Specifies the non-authentication policy for this VNS

Usage

When you create a VNS, if the referenced WLAN Service has a mode of:

- "std" then the referenced policy must have a topology of mode "b@ap," "b@ac," or "routed"
- "3pap" then the referenced policy must have a physical topology mode
- "wds" then the referenced policy must have a null topology

Examples

The following example creates a VNS named *testvns* and assigns it a WLAN Service named "HWC-1" and a policy named "NonAuth."

```
EWC.enterasys.com:vnsmode# create testvns wlans HWC-1 pol NonAuth
```

Note: After you run the **create** command, you must run the **apply** command to implement the changes.

18.3 das

Use the **das** command to configure DAS (Dynamic Authorization Server) settings. Executing the **das** command puts you in the **vnsmode:das** context where the following commands are available.

The following commands are available in the **vnsmode:das** context:

- port
- replay_interval

18.3.1 port

Use the **port** command to configure the DAS port. The **port** command is available from the **vnsmode:das** context.

Syntax

```
port <1024-65535>
```

Parameters

<1024-65535>	Specifies the DAS port.

Examples

The following example sets the DAS port number to 3799.

```
EWC.enterasys.com:vnsmode:das# port 3799
```

18.3.2 replay_interval

Use the **replay_interval** command to configure the DAS replay interval, measured in seconds. The **replay_interval** command is available from the **vnsmode:das** context.

Syntax

```
replay_interval <0-1000>
```

Parameters

<0-1000>	Specifies the DAS replay interval, measured in seconds.

Examples

The following example sets the DAS replay interval to 60 seconds.

```
EWC.enterasys.com:vnsmode:das# replay_interval 60
```

18.4 default-policy

The **default-policy** command moves you into the **vnsmode:default-policy** context. The **vnsmode:default-policy** context provides commands for the configuration of the default-policy.

The default-policy definitions provide a placeholder for completion of incomplete (no-change) policies for the VNS being configured. Refer to Chapter 20, **policy Commands** for a complete discussion of policy commands.

The default-policy specifies:

- A topology to use when a VNS is created using a policy (non-auth policy) that does not specify a topology. The default assigned topology is the Bridge Traffic Locally at AP topology.
- An inbound and outbound rate control profile. The default rate control profile is "Unlimited".
- A set of filters. The default filter set is a single deny all rule.

Note: After you have completed configuration changes for the default-policy, you must run the **apply** command before exiting the vnsmode:default-policy context to implement the changes.

The following commands are available in the **vnsmode:default-policy** context:

- show
- sync
- acfilters — See acfilters for commands in the **vnsmode:default-policy:acfilters** context.
- rateprf-in
- rateprf-out
- topology-name
- ulfilterap
- apcustom
- apfilters — See apfilters for commands in the **vnsmode:default-policy:apfilters** context.

18.4.1 show

Use the **show** command to display the default-policy configuration information for the current vnsmode:default-policy context. The **show** command is accessible from within the the vnsmode:default-policy context.

Syntax

```
show
```

Parameters

None.

Examples

The following example displays the default-policy configuration from within the vnsmode:default-policy context:

```
EWC.enterasys.com:vnsmode:default-policy#  show
Assigned topology: Bridged at AP untagged
```

```
Ingress rate profile: Unlimited
Egress rate profile: Unlimited
Enable AP filtering: enable
Synchronize: disable
EWC.enterasys.com:vnsmode:default-policy#
```

18.4.2 sync

Use the **sync** command to enable or disable automatic synchronization of the default-policy across paired controllers. Refer to the Enterasys Wireless Controller *User Guide* for more information about synchronization of policies.

The **sync** command is accessible from within the v**nsmode:default-policy** context.

Syntax

```
sync {enable | disable}
```

Parameters

enable | disable	Enables or disables synchronization of the default-policy across controllers.

Examples

The following example enables the synchronization of the default-policy across controllers:

```
EWC.enterasys.com:vnsmode:default-policy# sync enable
EWC.enterasys.com:vnsmode:default-policy# apply
EWC.enterasys.com:vnsmode:default-policy# show
Assigned topology: Bridged at AP untagged
Ingress rate profile: Unlimited
Egress rate profile: Unlimited
Enable AP filtering: disable
Synchronize: enable
EWC.enterasys.com:vnsmode:default-policy#
```

18.4.3 acfilters

Use the **acfilter**s command to enter the **vnsmode:default-policy:acfilters** context for the configuring of default-policy AC filters. The **acfilters** command is accessible from within the the vnsmode:default-policy context.

AC filter rules are applied at the controller. Default-policy AC filter configuration is applied when no AC filters are configured for policy applied at the controller.

Notes: AC filtering is not available when the associated topology is configured for Bridge at AP. AC filtering is available when the associated topology is set to either Bridge at AC or Routed.

The **acfilter** command has been replaced by **acfilters**. **acfilter** is deprecated.

The following commands are available in the **vnsmode:default-policy:acfilters** context:

- create

- config
- delete
- move

18.4.3.1 create

Use the **create** command to create, insert, or append a new filter rule into an AC filter list for the default-policy. The **create** command is accessible from within the **vnsmode:default-policy:acfilters** context.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode sytax:

```
create <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|dst) out (none|src)
(allow | deny)
```

Advanced mode syntax:

```
create <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|src|dst|both) out
(none|src|dst|both) (allow | deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <protocol>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **all** - All protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
<ipaddress/mask>	Specifies an IP address and mask for this filter rule.
interface-subnet	Specifies that the IP address and mask configured for the associated topology will be used for this filter rule.
interface-ip	Specifies the IP address of the associated topology will be used for this filter rule.
port <port> [<port>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.

type <type> [<type>]	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0 - 255.
Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow. — **in** specifies a packet flow from the AP to the AC (into network). **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
Basic: out (none|src) Advanced: out (none|src|dst|both)	Specifies the direction of packet flow. — **out** specifies a packet flow from the AC to the AP (out of network). **none** specifies that the **out** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
allow | deny	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified rule position already contains a filter rule, this command inserts a rule in the specified position in the list and resequences all other rules below this rule by one position. Use the **create** command to insert or append a rule at the specified list position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example creates a filter rule 1 that allows UDP traffic in both directions from the associated topology's interface-subnet for ports 10 through 2000:

```
EWC.enterasys.com:vnsmode:default-policy:acfilters# create 1 proto udp interface-
subnet port 10 2000 in dst out src allow
EWC.enterasys.com:vnsmode:default-policy:acfilters# apply
EWC.enterasys.com:vnsmode:default-policy:acfilters# show
Enable AP filtering: disable
filter 1 proto udp interface-subnet port 10 2000 in dst out src allow
filter 2 (default) proto none 0.0.0.0  all_ports in dst out src deny
EWC.enterasys.com:vnsmode:default-policy:acfilters#
```

The following example creates a filter rule 1 that is inserted into the rule list at position 1, resequencing the current rule 1. This filter rule allows TCP traffic in both directions from the associated topology's interface-subnet for ports 10 through 20000:

```
EWC.enterasys.com:vnsmode:default-policy:acfilters# create 1 proto tcp interface-subnet port 10 2000 in dst out src allow
EWC.enterasys.com:vnsmode:default-policy:acfilters# apply
EWC.enterasys.com:vnsmode:default-policy:acfilters# show
Enable AP filtering: disable
filter 1 proto tcp interface-subnet port 10 2000 in dst out src allow
filter 2 proto udp interface-subnet port 10 2000 in dst out src allow
filter 3 (default) proto none 0.0.0.0  all_ports in dst out src deny
EWC.enterasys.com:vnsmode:default-policy:acfilters#
```

18.4.3.2 config

Use the **config** command to modify an existing AC filter rule for the default-policy. The **config** command is accessible from within the **vnsmode:default-policy:acfilters** context.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode syntax:

```
config <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip) [(port <port> [<port>]) | (type <type> [<type>])] in (none|dst) out (none|src) (allow|deny)
```

Advanced mode syntax:

```
config <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip) [(port <port> [<port>]) | (type <type> [<type>])] in (none|src|dst|both) out (none|src|dst|both) (allow|deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <protocol>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **all** - All protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
<ipaddress/mask>	Specifies an IP address and mask for this filter.
interface-subnet	Specifies that the IP address and mask configured for the associated topology will be used for this filter rule.

interface-ip	Specifies the IP address of the associated topology will be used for this filter rule.
port <port> [<port>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a port range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type <type> [<type>]	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0 - 255.
Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow. — **in** specifies a packet flow from the AP to the AC (into the network). **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
Basic: out (none|src) Advanced: out (none|src|dst|both)	Specifies the direction of packet flow. — **out** specifies a packet flow from the AC to the AP (out of the network). **none** specifies that the **out** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
allow | deny	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified rule position already contains a filter rule, the **config** command overwrites the existing rule. Use the **create** command to insert or append a rule at the specified position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example overwrites a pre-existing filter rule 1 with a rule that allows ICMP traffic types 9 through 31 in both directions for the associated topology's:

```
EWC.enterasys.com:vnsmode:default-policy:acfilters# config 1 proto icmp
interface-subnet type 9 31 in dst out src allow
EWC.enterasys.com:vnsmode:default-policy:acfilters# apply
EWC.enterasys.com:vnsmode:default-policy:acfilters# show
```

```
Enable AP filtering: disable
filter 1 proto icmp interface-subnet type 9 31 in dst out src allow
filter 2 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src allow
filter 3 (default) proto none 0.0.0.0  all_ports in dst out src deny
EWC.enterasys.com:vnsmode:default-policy:acfilters#
```

18.4.3.3 delete

Use the **delete** command to remove a filter rule from the filter list. The **delete** command is accessible from within the **vnsmode:default-policy:acfilters** context.

Syntax

```
delete <pos>
```

Parameters

<pos>	Specifies the filter rule list position of the filter rule to be deleted. Valid values are from 0 - 255.

Examples

The following example deletes filter rule 1 and displays the remaining default deny all rule:

```
EWC.enterasys.com:vnsmode:default-policy:acfilters# delete 1
EWC.enterasys.com:vnsmode:default-policy:acfilters# show
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0  all_ports both deny
```

18.4.3.4 move

Use the **move** command to move a filter rule from its current position in the filter list to the specified filter list position. The **move** command is accessible from within the **vnsmode:default-policy:acfilters** context.

Syntax

```
move <cur-pos> <new-pos>
```

Parameters

<cur-pos> <new-pos>	Specifies the current position in the filter list of the rule to be moved, followed by the new list position for the filter rule. Valid values are from 0 - 255.

Examples

The following example:

- Moves the rule in list position 2 to list position 1
- Displays the new list ordering:

```
EWC.enterasys.com:vnsmode:default-policy:acfilters# move 2 1
EWC.enterasys.com:vnsmode:default-policy:acfilters# show
```

```
Enable AP filtering: disable
filter 1 proto udp 192.168.10.0 255.255.255.0 port 10 2000 both allow
filter 2 proto icmp interface-subnet type 9 31 both allow
filter 3 (default) proto none 0.0.0.0  all_ports both deny
EWC.enterasys.com:vnsmode:default-policy:acfilters#
```

18.4.4 rateprf-in

Use the **rateprf-in** command to associate an already existing rate profile for a policy as an ingress rate profile. The **rateprf-in** command is accessible from the **vnsmode:default-policy** context.

Syntax

```
rateprf-in <profile>
```

Parameters

<profile>	Specifies the ingress rate profile to configure for this vnsmode:default-policy context.

Usage

Refer to "rateprofile" on page 18-32 for rate profile configuration information.

Examples

The following example configures the default-policy with the **Unlimited** ingress rate profile:

```
EWC.enterasys.com:vnsmode:default-policy# rateprf-in DocRateIn
EWC.enterasys.com:vnsmode:default-policy# apply
EWC.enterasys.com:vnsmode:default-policy# show
Assigned topology: guestPortal
Ingress rate profile: DocRateIn
Egress rate profile: Unlimited
Enable AP filtering: disable
Synchronize: enable
EWC.enterasys.com:vnsmode:default-policy#
```

18.4.5 rateprf-out

Use the **rateprf-out** command to associate an already existing rate profile for a policy as an egress rate profile. The **rateprf-out** command is accessible from the **vnsmode:default-policy** context.

Syntax

```
rateprf-out <profile>
```

Parameters

<profile>	Specifies the egress rate profile to configure for this vnsmode:default-policy context.

Usage

Refer to "rateprofile" on page 18-32 for Rate Profile Configuration Information.

Examples

The following example configures the default-policy with the **Unlimited** egress rate profile:

```
EWC.enterasys.com:vnsmode:default-policy# rateprf-out DocRateOut
EWC.enterasys.com:vnsmode:default-policy# apply
EWC.enterasys.com:vnsmode:default-policy# show
Assigned topology: guestPortal
Ingress rate profile: DocRateIn
Egress rate profile: DocRateOut
Enable AP filtering: disable
Synchronize: enable
EWC.enterasys.com:vnsmode:default-policy#
```

18.4.6 topology-name

Use the **topology-name** command to associate an already existing topology with a policy. The **topology-name** command is accessible from the **vnsmode:default-policy** context.

Syntax

```
topology-name <topology>
```

Parameters

<topology>	Specifies the name of the topology to configure for this vnsmode:default-policy context.

Usage

Refer to Chapter 21, **topology Commands** for information on configuring topologies.

Examples

The following example configures the default-policy with the **guestPortal** topology:

```
EWC.enterasys.com:vnsmode:default-policy# topology-name guestPortal
EWC.enterasys.com:vnsmode:default-policy# apply
EWC.enterasys.com:vnsmode:default-policy# show
Assigned topology: guestPortal
Ingress rate profile: Unlimited
Egress rate profile: Unlimited
Enable AP filtering: disable
Synchronize: enable
EWC.enterasys.com:vnsmode:default-policy#
```

18.4.7 ulfilterap

Use the **ulfilterap** command to enable filtering on the AP. The **ulfilterap** command is accessible from the **vnsmode:default-policy** context.

Syntax

```
ulfilterap {enable | disable}
```

Parameters

enable | disable	Provides for the enabling or disabling of filtering on the AP for this vnsmode:default-policy context.

Usage

When filtering is enabled on the AP, wireless APs obtain client filter information from the Enterasys Wireless Controller. Filter rules defined on the controller are applied by wireless APs. In addition, direct inter-Wireless AP communication allows Wireless APs to exchange client filter information as clients roam from one Wireless AP to another.

Enabling filtering on the AP provides for the ability to apply custom filters for the AP using the **apcustom** command.

Examples

The following example enables filtering on the AP for this vnsmode:default-policy context:

```
EWC.enterasys.com:vnsmode:default-policy# ulfilterap enable
EWC.enterasys.com:vnsmode:default-policy# show
Assigned topology: guestPortal
Ingress rate profile: Unlimited
Egress rate profile: Unlimited
Enable AP filtering: enable
Custom AP Filters: disable
Synchronize: enable
EWC.enterasys.com:vnsmode:default-policy#
```

18.4.8 apcustom

Use the **apcustom** command to enable configuring AP custom filters. The **apcustom** command is accessible from the **vnsmode:default-policy** context.

Syntax

```
apcustom {enable | disable}
```

Parameters

enable | disable	Provides for the enabling or disabling of AP custom filters for this vnsmode:default-policy context.

Usage

Enabling AP custom filters allows you to access the **vnsmode:default-policy: apfilters** context by executing the **apfilters** command. The **vnsmode:default-policy:apfilters** context allows you to configure additional filters for the APs.

Filtering on the AP must be enabled using the **ulfilterap enable** command for the **apcustom** command to be visible in the CLI. The **apcustom enable** command makes the **apfilters** command visible.

Examples

The following example enables AP custom filters:

```
EWC.enterasys.com:vnsmode:default-policy# ulfilterap enable
EWC.enterasys.com:vnsmode:default-policy# apcustom enable
EWC.enterasys.com:vnsmode:default-policy# apfilters
EWC.enterasys.com:vnsmode:default-policy:apfilters#
```

18.4.9 apfilters

Use the **apfilters** command to enter the **vnsmode:default-policy:apfilters** context for the configuring of AP custom filters. AP custom filters are applied at the AP. Default-policy AP custom filters are applied when no AP custom filters are configured for policy applied at the AP. The **apfilters** command is accessible from the **vnsmode:default-policy** context.

This command is not visible in the CLI if you execute the **apcustom disable** command.

Note: The **apfilter** command has been replaced by the **apfilters** command. **apfilter** is deprecated.

The following commands are available in the **vnsmode:default-policy:apfilters** context:

- create
- config
- delete
- move

18.4.9.1 create

Use the **create** command to create, insert, or append a new AP filter rule for this default-policy. The **create** command is accessible from the **vnsmode:default-policy:apfilters** context.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode syntax:

```
create <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|dst) out (none|src)
(allow | deny)
```

Advanced mode syntax:

```
create <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|src|dst|both) out
(none|src|dst|both) (allow | deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <protocol>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **all** - All protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
<ipaddress/mask>	Specifies an IP address and mask for this filter.
interface-mask	Specifies that the IP address and mask configured for the associated topology will be used for this filter rule.
interface-ip	Specifies the IP address of the associated topology will be used for this filter rule.
port <port> [<port>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type <type> [<type>]	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0 - 255.
Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow. — **in** specifies a packet flow from the AP to the AC (into network). **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.

Basic: out (none|src) Advanced: out (none|src|dst|both)	Specifies the direction of packet flow. — **out** specifies a packet flow from the AC to the AP (out of network). **none** specifies that the **out** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
allow | deny	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified rule position already contains a filter rule, specifying a rule using this command inserts a rule in the currently existing rules position and resequences all other rules below this rule by one position. Use the **create** command to insert or append a rule at the specified position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example creates a filter rule 1 that allows UDP traffic in both directions from subnet 10.10.10.0/24 for ports 10 through 2000:

```
EWC.enterasys.com:vnsmode:default-policy:apfilters# create 1 proto udp
10.10.10.0/24 port 10 2000 in dst out src allow
EWC.enterasys.com:vnsmode:default-policy:apfilters# show
Custom AP Filters: enable
filter 1 proto udp 10.10.10.0 255.255.255.0 port 10 2000 in dst out src allow
filter 2 (default) proto none 0.0.0.0  all_ports in dst out src deny
EWC.enterasys.com:vnsmode:default-policy:apfilters#
```

The following example creates a filter rule 1 that is inserted into the rule list at position 1 because a rule already exists for rule 1. This filter rule allows ICMP types 9 through 31 traffic in both directions from IP address 20.20.0.0/16:

```
EWC.enterasys.com:vnsmode:default-policy:apfilters# create 1 proto icmp
20.20.0.0/16 type 9 31 in dst out src allow
EWC.enterasys.com:vnsmode:default-policy:apfilters# show
Custom AP Filters: enable
filter 1 proto icmp 20.20.0.0 255.255.0.0 type 9 31 in dst out src allow
filter 2 proto udp 10.10.10.0 255.255.255.0 port 10 2000 in dst out src allow
filter 3 (default) proto none 0.0.0.0  all_ports both deny
EWC.enterasys.com:vnsmode:default-policy:apfilters#
```

18.4.9.2 config

Use the **config** command to modify an existing AP filter rule for the default-policy. The **config** command is accessible from the **vnsmode:default-policy:apfilters** context.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode syntax:

```
config <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|dst) out (none|src)
(allow|deny)
```

Advanced mode syntax:

```
config <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|src|dst|both) out
(none|src|dst|both) (allow|deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <protocol>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **all** - All protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
<ipaddress/mask>	Specifies an IP address and mask for this filter.
interface-subnet	Specifies the IP address and mask configured for the associated topology.
interface-ip	Specifies the IP address of the associated topology
port <port> [<port>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type <type> [<type>]	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0 - 255.

Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow. — **in** specifies a packet flow from the AP to the AC (into the network). **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
Basic: out (none|src) Advanced: out (none|src|dst|both)	Specifies the direction of packet flow. — **out** specifies a packet flow from the AC to the AP (out of the network). **none** specifies that the **out** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
allow | deny	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified rule position already contains a filter rule, this command overwrites the existing rule. Use the **create** command to insert or append a rule at the specified position.

Examples

The following example overwrites a pre-existing filter rule 1 with a rule that allows ICMP traffic types 9 through 31 in both directions for the associated topology's:

```
EWC.enterasys.com:vnsmode:default-policy:apfilters# config 1 proto icmp
interface-subnet type 9 31 both allow
EWC.enterasys.com:vnsmode:default-policy:apfilters# apply
EWC.enterasys.com:vnsmode:default-policy:apfilters# show
Custom AP Filters: enable
filter 1 proto icmp interface-subnet type 9 31 both allow
filter 2 proto udp 10.10.10.0 255.255.255.0 port 20 2000 both allow
filter 3 (default) proto none 0.0.0.0  all_ports both deny
EWC.enterasys.com:vnsmode:default-policy:apfilters#
```

18.4.9.3 delete

Use the **delete** command to remove a filter rule from the AP filter list. The **delete** command is accessible from the **vnsmode:default-policy:apfilters** context.

Syntax

```
delete <pos>
```

Parameters

<pos>	Specifies the filter rule list position of the filter to be deleted. Valid values are from 0 - 255.

Examples

The following example deletes filter rule 1 and displays the remaining deny all rule:

```
EWC.enterasys.com:vnsmode:default-policy:apfilters# delete 1
EWC.enterasys.com:vnsmode:default-policy:apfilters# show
Custom AP Filters: enable
filter 1 (default) proto none 0.0.0.0  all_ports both deny
EWC.enterasys.com:vnsmode:default-policy:apfilters#
```

18.4.9.4 move

Use the **move** command to move a filter rule from its current position in the filter list to the specified filter list position. The **move** command is accessible from the **vnsmode:default-policy:apfilters** context.

Syntax

```
move <cur-pos> <new-pos>
```

Parameters

<cur-pos> <new-pos>	Specifies the current position in the filter list of the rule to be moved, followed by the new list position for the filter rule. Valid values are from 0 - 255.

Examples

The following example:

- Moves the rule in list position 2 to list position 1
- Displays the new list ordering :

```
EWC.enterasys.com:vnsmode:default-policy:apfilters# move 2 1
EWC.enterasys.com:vnsmode:default-policy:apfilters# show
Custom AP Filters: enable
filter 1 proto udp interface-subnet port 20 2000 both allow
filter 2 proto icmp interface-subnet type 9 31 both allow
filter 3 (default) proto none 0.0.0.0  all_ports both deny
EWC.enterasys.com:vnsmode:default-policy:apfilters#
```

18.5 delete

Use the **delete** command in **vnsmode** to delete an existing VNS.

Syntax

```
delete <VNS name>
```

Parameters

<VNS name>	Specifies the VNS to delete.

Examples

The following example deletes the VNS named guestportal.

```
EWC.enterasys.com:vnsmode:delete guestportal
```

18.6 radius

Executing the **radius** command moves you into the **vnsmode:radius** context, which contains the following commands to manage RADIUS server configuration. After you create a radius server configuration, you can further configure it by entering the **vnsmode:radius:<server-name>** context. See "<named_RADIUS_server>" on page 18-27.

The following commands are available in the **vnsmode:radius** context:

- create
- delay-client-msg
- delete
- include-service-type
- show
- radius-mac-format
- rename
- strict
- <named_RADIUS_server> — See <named_RADIUS_server> for commands in the **vnsmode:radius:<server-name>** context.

18.6.1 create

Use the **create** command to create a RADIUS server configuration. The **create** command is accessible from the **vnsmode:radius** context of the CLI.

Syntax

```
create <name> A.B.C.D <secret>
```

Parameters

<name>	Specifies the name of the RADIUS server
A.B.C.D	Specifies the IP address of the RADIUS server
<secret>	Specifies the shared secret for the RADIUS server

Examples

The following example creates and then displays the details of a RADIUS server configuration named test-radius-server with an IP address of 10.10.10.10 and a shared secret of "test."

```
EWC.enterasys.com:vnsmode:radius# create test-radius-server 10.10.10.10 test
EWC.enterasys.com:vnsmode:radius# test-radius-server
EWC.enterasys.com:vnsmode:radius:test-radius-server# show
Authentication port: 1812
Accounting port: 1813
Authentication priority: 5
Accounting priority: 5
Authentication total number of tries: 3
Accounting total number of tries: 3
Authentication RADIUS request timeout: 5
Accounting RADIUS request timeout: 5
Interim accounting interval: 0
Default protocol: PAP
Shared secret: ****
Name: test-radius-server
```

18.6.2 delay-client-msg

Use the **delay-client-msg** command to set the delay, in seconds, for the client message that displays if a topology change occurs during athentication. The **delay-client-msg** command is accessible from the **vnsmode:radius** context of the CLI.

Syntax

```
delay-client-msg <1-60>
```

Parameters

<1-60>	The time, in seconds, that the client message displays if a topology change occurs during athentication.

Examples

The following example sets the delay to 40 seconds.

```
EWC.enterasys.com:vnsmode:radius# delay-client-msg 40
```

18.6.3 delete

Use the **delete** command to delete a RADIUS server configuration. The **delete** command is accessible from the **vnsmode:radius** context of the CLI.

Syntax

```
delete <RADIUS_server>
```

Parameters

<RADIUS_server>	Specifies the name of the RADIUS server to delete

Examples

The following example deletes the RADIUS server named test-radius-server.

```
EWC.enterasys.com:vnsmode:radius# delete test-radius-server
```

18.6.4 include-service-type

Use the **include-service-type** command to include or exclude the Serice-Type attribute in the client Access-Request message. The **include-service-type** command is accessible from the **vnsmode:radius** context of the CLI.

Syntax

```
include-service-type enable|disable
```

Parameters

enable	Include the Service-Type attribute in the client Access-Request message.
disable	Exclude the Service-Type attribute from the client Access-Request message.

Examples

```
EWC.enterasys.com:vnsmode:radius# inlcude-service-type enable
```

18.6.5 show

Use the **show** command to display RADIUS server configuration information. The **show** command is accessible from the **vnsmode:radius** context of the CLI.

Syntax

```
show [<RADIUS_server>]
```

Parameters

<RADIUS_server>	Specifies to display information about the specific RADIUS server

Examples

The following example displays a list of RADIUS server configuration information.

```
EWC.enterasys.com:vnsmode:radius# show
Strict: disable
Radius MAC format: 1. XXXXXXXXXXX
Client Access-Request includes Service-Type Attribute: disable

Name      IP address   Protocol  Retries(Auth:Acct)  Timeout(Auth:Acct)  Ports(Auth:Acct)
Priority(Auth:Acct)

RADIUS_1  192.0.1.202  PAP       3:3                 5:5                 1812:1813         1:1
```

The following example displays configuration information for the RADIUS server named "RADIUS_1."

```
EWC.enterasys.com:vnsmode:radius# show RADIUS_1
Authentication port: 1812
Accounting port: 1813
Authentication priority: 1
Accounting priority: 1
Authentication total number of tries: 3
Accounting total number of tries: 3
Authentication RADIUS request timeout: 5
Accounting RADIUS request timeout: 5
Interim accounting interval: 30
Default protocol: PAP
Shared secret: **********
Name: RADIUS_1
Radius IP: 192.0.1.202
```

18.6.6 radius-mac-format

Use the **radius-mac-format** command to set the MAC address format to be exchanged with the RADIUS server. The **radius-mac-format** command is accessible from the **vnsmode:radius** context of the CLI.

Syntax

```
radius-mac-format {1|2|3|4|5|6|101|102|103|104|105|106}
```

Parameters

1	Specifies a MAC address format of XXXXXXXXXXX for use with the RADIUS server
2	Specifies a MAC address format of XX:XX:XX:XX:XX:XX for use with the RADIUS server
3	Specifies a MAC address format of XX-XX-XX-XX-XX-XX for use with the RADIUS server
4	Specifies a MAC address format of XXXX.XXXX.XXXX for use with the RADIUS server

5	Specifies a MAC address format of XXXXXX-XXXXXX for use with the RADIUS server
6	Specifies a MAC address format of XX XX XX XX XX XX for use with the RADIUS server
101	Specifies a MAC address format of xxxxxxxxxxxx for use with the RADIUS server
102	Specifies a MAC address format of xx:xx:xx:xx:xx:xx for use with the RADIUS server
103	Specifies a MAC address format of xx-xx-xx-xx-xx-xx for use with the RADIUS server
104	Specifies a MAC address format of xxxx.xxxx.xxxx for use with the RADIUS server
105	Specifies a MAC address format of xxxxxx-xxxxxx for use with the RADIUS server
106	Specifies a MAC address format of xx xx xx xx xx xx for use with the RADIUS server

Examples

The following example sets the RADIUS MAC address format to XX:XX:XX:XX:XX:XX

```
EWC.enterasys.com:vnsmode:radius# radius-mac-format 2
```

Note: After you run the **radius-mac-format** command, you must run the **apply** command to implement the changes.

18.6.7 rename

Use the **rename** command to rename the RADIUS server. The **rename** command is accessible from the **vnsmode:radius** context of the CLI.

Syntax

```
rename <radius-name> new-name <new-name>
```

Parameters

<radius-name>	Specifies the existing name of the RADIUS server
new-name	Identifies that the following characters are to be the new name for the RADIUS server
<new-name>	Specifies the new name of the RADIUS server

Examples

The following example renames the RADIUS server ADV to IAV.

```
EWC.enterasys.com:vnsmode:radius# rename ADV new-name IAV
```

18.6.8 strict

Use this command to enable or disable the ability to change RADIUS server settings per WLAN Service. This command is available from the **vnsmode:radius** context.

Syntax

```
strict <enable | disable>
```

Parameters

enable	Enables changing RADIUS server settings per WLAN Service.
disable	Disables changing RADIUS server settings per WLAN Service.

Examples

This example disables changing RADIUS server settings per WLAN Service.

```
EWC.enterasys.com:vnsmode:radius# strict disable
```

18.6.9 <named_RADIUS_server>

The **<named_RADIUS_server>** command, where <named_RADIUS_server> refers to the name of a given RADIUS server, is available in the **vnsmode:radius** context. When executed, it moves you into the **vnsmode:radius:<named_ RADIUS_server>** context, which contains commands to configure the settings of the specified individual RADIUS server.

The following commands are available in the **vnsmode:radius:<named_ RADIUS_server>** context:

- acct-port
- acct-prio
- acct-retries
- acct-timeout
- auth-port
- auth-prio
- auth-retries
- auth-timeout
- interim
- ip
- name
- protocol
- shared-secret

18.6.9.1 acct-port

Use the **acct-port** command to set the port for RADIUS accounting. The **acct-port** command is accessible from the **vnsmode:radius:<named_RADIUS _server>** context of the CLI.

If you do not change the port with this command, the default port 1813 is used.

Syntax

```
acct-port <0-65535>
```

Parameters

<0-65535>	Specifies the RADIUS accounting port

The following example sets the RADIUS accounting port to 1646 for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# acct-port 1646
```

18.6.9.2 acct-prio

Use the **acct-prio** command to set the priority for RADIUS accounting. The **acct-prio** command is accessible from the **vnsmode:radius:<named_RADIUS _server>** context of the CLI.

Syntax

```
acct-prio <0-32>
```

Parameters

<0-32>	Specifies the RADIUS accounting priority

The following example sets the RADIUS accounting priority to 12 for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# acct-prio 12
```

18.6.9.3 acct-retries

Use the **acct-retries** command to set the the total number of RADIUS accounting attempts. The **acct-retries** command is accessible from the **vnsmode:radius: <named_RADIUS_server>** context of the CLI.

Syntax

```
acct-retries <1-32>
```

Parameters

<1-32>	Specifies the total number of RADIUS accounting attempts.

Examples

The following example sets the number of RADIUS accounting retries to 5 for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# acct-retries 5
```

18.6.9.4 acct-timeout

Use the **acct-timeout** command to set the timeout for RADIUS accounting. The **acct-timeout** command is accessible from the **vnsmode:radius:<named_ RADIUS_server>** context of the CLI.

Syntax

```
acct-timeout <1-360>
```

Parameters

<1-360>	Specifies the RADIUS accounting timeout in seconds.

Examples

The following example sets the RADIUS accounting timeout to 10 seconds for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# acct-timeout 10
```

18.6.9.5 auth-port

Use the **auth-port** command to set the priority for RADIUS authentication. The **auth-port** command is accessible from the **vnsmode:radius:<named_ RADIUS_server>** context of the CLI. If you do not change the authentication port number with this command, the controller uses the default port 1812.

Syntax

```
auth-port <0-65535>
```

Parameters

<0-65535>	Specifies the RADIUS authentication port.

Examples

The following example sets the port for RADIUS authentication to port 1816 for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# auth-port 1816
```

18.6.9.6 auth-prio

Use the **auth-prio** command to set the priority for RADIUS authentication. The **auth-prio** command is accessible from the **vnsmode:radius:<named_ RADIUS_server>** context of the CLI.

Syntax

```
auth-prio <0-32>
```

Parameters

<0-32>	Specifies the RADIUS authentication priority.

Examples

The following example sets the RADIUS authentication priority to 5 for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# auth-prio 5
```

18.6.9.7 auth-retries

Use the **auth-retries** command to set the the total number of RADIUS authentication attempts. The **auth-retries** command is accessible from the **vnsmode:radius: <named_RADIUS_server>** context of the CLI.

Syntax

```
auth-retries <1-32>
```

Parameters

<1-32>	Specifies the total number of RADIUS authentication attempts.

Examples

The following example sets the number of RADIUS authentication attempts to 5 for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# auth-retries 5
```

18.6.9.8 auth-timeout

Use the **auth-timeout** command to set the timeout for RADIUS authentication. The **auth-timeout** command is accessible from the **vnsmode:radius:<named_ RADIUS_server>** context of the CLI.

Syntax

```
auth-timeout <1-360>
```

Parameters

<1-360>	Specifies the RADIUS authentication timeout in seconds.

Examples

The following example sets the RADIUS authentication timeout to 10 seconds for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# auth-timeout 10
```

18.6.9.9 interim

Use the **interim** command to set the RADIUS interim accounting interval. The **interim** command is accessible from the **vnsmode:radius:<named_RADIUS_ server>** context of the CLI.

Syntax

```
interim <0-360>
```

Parameters

<0-360>	Specifies the RADIUS interim accounting interval in seconds.

Examples

The following example sets the RADIUS interim accounting interval to 10 seconds for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# interim 10
```

18.6.9.10 ip

Use the **ip** command to configure the IP address of the RADIUS server. The **ip** command is accessible from the **vnsmode:radius:<named_RADIUS_server>** context of the CLI.

Syntax

```
ip A.B.C.D
```

Parameters

A.B.C.D	Specifies the IP address of the RADIUS server in dotted decimal notation.

Examples

The following example sets the IP address of the IAS RADIUS server to 222.224.1.23.

```
EWC.enterasys.com:vnsmode:radius:RAD1# ip 222.224.1.23
```

18.6.9.11 name

Use the **name** command to modify the RADIUS server name. The **name** command is accessible from the **vnsmode:radius:<named_RADIUS_server>** context of the CLI.

Syntax

```
name <new_RADIUS_server_name>
```

Parameters

<new_RADIUS_server_name>	Specifies the name of the RADIUS server.

Examples

The following example renames the RADIUS server RAD1 to RAD2.

```
EWC.enterasys.com:vnsmode:radius:RAD1# name RAD2
EWC.enterasys.com:vnsmode:radius:RAD1# show name
Name: RAD2
```

18.6.9.12 protocol

Use the **protocol** command to set the security protocol used with the RADIUS server. The **protocol** command is accessible from the **vnsmode:radius: <named_RADIUS_server>** context of the CLI.

Syntax

```
protocol [CHAP|MS-CHAP|MS-CHAP2|PAP]
```

Parameters

CHAP|MS-CHAP|MS-CHAP2|PAP	Specifies the security protocol that is used between the RADIUS Server and the Enterasys Wireless Controller

Examples

The following example sets the security protocol to PAP for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# protocol PAP
```

18.6.9.13 shared-secret

Use the **shared-secret** command to set the shared secret used with the RADIUS server. The **shared-secret** command is accessible from the **vnsmode:radius:<named_RADIUS_server>** context of the CLI.

Syntax

```
shared-secret <shared secret>
```

Parameters

<shared secret>	Specifies the shared secret that is used between the RADIUS Server and the Enterasys Wireless Controller

Examples

The following example sets the shared secret to "hwc" for the RADIUS server named RAD1.

```
EWC.enterasys.com:vnsmode:radius:RAD1# shared-secret hwc
```

18.7 rateprofile

Executing the **rateprofile** command moves you into the **vnsmode:rateprofile** context, which contains the following commands to manage bandwidth rate control profiles.

The following commands are available in the **vnsmode:rateprofile** context:

- create
- delete
- show

18.7.1 create

Use the **create** command to create a bandwidth rate control profile with an average rate in Kbps. The **create** command is accessible from the **vnsmode:rateprofile** context of the CLI.

In the **vnsmode:rateprofile** context, use the delete command to delete a bandwidth rate control profile, and use the **show** command to display existing rate control profiles.

Note: You can create up to 128 profiles.

Syntax

```
create <profile_name> <average rate>
```

Parameters

<profile_name>	Specifies the name of the rate control profile
<average rate>	Specifies committed information rate (CIR) in Kbps.

Examples

The following example creates a bandwidth rate control profile named lowspeed with 200 Kbps of CIR.

```
EWC.enterasys.com:vnsmode:rateprofile# create lowspeed 200
```

Note: Average Rate (CIR) must be between 128 and 200000 (kbps).

The following example creates a bandwidth rate control profile named high speed with 700 Kbps of CIR.

```
EWC.enterasys.com:vnsmode:rateprofile# create “high speed” 700
```

Note: If you are using a profile name that consists of two words and the two words are separated by space, you must put the profile name in double quotes (“).

Note: After you run the **create** command, you must run the **apply** command to implement the changes.

18.7.2 delete

Use the **delete** command to delete a bandwidth rate control profile. The **delete** command is accessible from the **vnsmode:rateprofile** context of the CLI.

Syntax

```
delete <profile_name>
```

Parameters

<profile_name>	Specifies the name of the bandwidth rate control profile to delete.

Delete rate profile

The following example deletes the lowspeed profile.

```
EWC.enterasys.com:vnsmode:rateprofile# delete lowspeed
```

Note: If the rate control profile that you are attempting to delete is being used by any other VNS, the system returns the following message: **You can not delete this profile because it is used by other VNS**.

18.7.3 show

Use the **show** command to display all existing bandwidth rate control profiles or a specific profile.

Syntax

```
show [<profile_name>]
```

Parameters

<profile_name>	Specifies the name of a specific rate control profile to display.

Examples

The following example displays all existing rate control profiles.

```
EWC.enterasys.com:vnsmode:rateprofile# show
Unlimited,0
lowspeed,200
```

18.8 <named-VNS>

Executing the **<named-VNS>** command, where <named-VNS> refers to the name of a configured VNS, moves you into the **vnsmode:<named-VNS>** context, which contains commands to configure the settings of the specified individual VNS.

The following commands are available in the **vnsmode:<named-VNS>** context:

- auth
- non-auth
- name
- pre-auth
- restrict
- status
- sync
- wlans-name
- show

18.8.1 auth

Use the **auth** command to assign a default policy for authenticated clients. This command is available from the **vnsmode:<named-VNS>** context.

Syntax

```
auth {non-auth | <policy-name>
```

Parameters

non-auth	Use the default policy for non-authenticated clients for authenticated clients.
<policy-name>	Specifies the name of the policy to use as the default policy for authenticated clients.

Usage

When you assign a default authenticated policy to this VNS, the same rules apply as when a VNS is created. That is — if the VNS's WLAN Service has a mode of:

- "std" then the referenced policy must have a topology of mode "b@ap," "b@ac," or "routed"
- "3pap" then the referenced policy must have a physical topology mode
- "wds" then the referenced policy must have a null topology

Examples

The following example specifies that the policy named "auth-users" should be used as the default policy for authenticated users for the VNS named VNS1.

```
EWC.enterasys.com:vnsmode:VNS1# auth auth-users
```

This example specifies that the same policy used as the default policy for non-authenticated users should be used for authenticated users for the VNS named VNS1.

```
EWC.enterasys.com:vnsmode:VNS1# auth non-auth
EWC.enterasys.com:vnsmode:VNS1# apply
```

Note: After you run the **auth** command, you must run the **apply** command to implement the changes.

18.8.2 non-auth

Use the **non-auth** command to change the default policy for non-authenticated clients. This command is available from the **vnsmode:<named-VNS>** context.

Syntax

```
non-auth <policy-name>
```

Parameters

<policy-name>	Specifies the name of the policy to use as the default policy for non-authenticated clients.

Usage

When you change the default non-authenticated policy for this VNS, the same rules apply as when a VNS is created. That is — if the VNS's WLAN Service has a mode of:

- "std" then the referenced policy must have a topology of mode "b@ap," "b@ac," or "routed"
- "3pap" then the referenced policy must have a physical topology mode
- "wds" then the referenced policy must have a null topology

Examples

The following example specifies that the policy named "non-auth-users" should be used as the default policy for non-authenticated users for the VNS named VNS1.

```
EWC.enterasys.com:vnsmode:VNS1# non-auth non-auth-users
EWC.enterasys.com:vnsmode:VNS1# apply
```

Note: After you run the **non-auth** command, you must run the **apply** command to implement the changes.

18.8.3 name

Use the **name** command in the **vnsmode:<named-VNS>** context to change the name of the current VNS.

Syntax

```
name <VNS-name>
```

Parameters

<VNS-name>	Specifies the new name for the current VNS.

Examples

The following example changes the name of VNS1 to VNS2, then uses the **show** command to display information for the current VNS, including its name.

```
EWC.enterasys.com:vnsmode:VNS1# name VNS2
EWC.enterasys.com:vnsmode:VNS1# apply
EWC.enterasys.com:vnsmode:VNS1# show
WLANS service: test
Non-authenticated: p4
Authenticated: same as non-authenticated
Restrict available policy set: disable
Enable status: enable
Synchronize: disable
Name: VNS2
```

Note: After you run the **name** command, you must run the **apply** command to implement the changes.

18.8.4 pre-auth

Use the **pre-auth** command to assign the default policy for pre-authenticated clients when the WLAN Service assigned to this VNS is configured with the **3pap** (3rd party AP) mode. The referenced policy can only reference a Topology of mode **physical**. This command is available in the **vnsmode:<named-VNS>** context.

Syntax

```
pre-auth <policy-name> | non-auth
```

Parameters

<policy-name>	Specifies the name of the policy to be applied to pre-authenticated clients.
non-auth	Use the default policy for non-authenticated clients for pre-authenticated clients.

Examples

The following example sets the policy for pre-authenticated clients to the default policy for non-authenticated clients.

```
EWC.enterasys.com:vnsmode:Wireless# pre-auth non-auth
EWC.enterasys.com:vnsmode:Wireless# show
WLANS service: 3rd
Non-authenticated: WirelessNonAuthPolicy
Authenticated: WirelessAuthPolicy
Pre-authenticated: same as non-authenticated
Restrict available policy set: disable
Enable status: disable
Synchronize: disable
Name: Wireless
```

18.8.5 restrict

Use the **restrict** command in the **vnsmode:<named-VNS>** context to enable or disable the "Restrict Policy Set" feature for this VNS. You can enable the "Restrict Policy Set" feature for VNSs that were configured prior to V7.0 and upgraded to V7.0 if you want the controller to respect the pre-V7.0 policy representation and to map external references to properly named policy representations created during upgrade.

Syntax

```
restrict (enable | disable)
```

Parameters

enable	Enables the "Restrict Policy Set" feature.
disable	Disables the "Restrict Policy Set" feature.

Examples

This example enables the Restrict Policy Set feature for the VNS named VNS1.

```
EWC.enterasys.com:vnsmode:VNS1# restrict enable
EWC.enterasys.com:vnsmode:VNS1# apply
```

Note: After you run the **restrict** command, you must run the **apply** command to implement the changes.

18.8.6 status

Use the **status** command in the **vnsmode:<named-VNS>** context to enable or disable the current VNS.

Syntax

```
status (enable | disable)
```

Parameters

enable	Enables the VNS.
disable	Disables the VNS.

Examples

This example disables the current VNS named VNS1.

```
EWC.enterasys.com:vnsmode:VNS1# status disable
EWC.enterasys.com:vnsmode:VNS1# apply
```

Note: After you run the **status** command, you must run the **apply** command to implement the changes.

18.8.7 sync

Use the **sync** command in the **vnsmode:<named-VNS>** context to enable or disable automatic synchronization of this VNS across paired controllers. Refer to the Enterasys Wireless Controller *User Guide* for more information about synchronization of VNSs.

Syntax

```
sync (enable | disable)
```

Parameters

enable	Enables automatic synchronization of this VNS across paired controllers.
disable	Disables automatic synchronization of this VNS.

Examples

This example enables automatic synchronization of the current VNS, named VNS1, across paired controllers.

```
EWC.enterasys.com:vnsmode:VNS1# sync enable
EWC.enterasys.com:vnsmode:VNS1# apply
```

Note: After you run the **sync** command, you must run the **apply** command to implement the changes.

18.8.8 wlans-name

Use the **wlans-name** command in the **vnsmode:<named-VNS>** context to associate a different WLAN Service with the current VNS. Only one WLAN Service can be associated with a VNS at a time.

Syntax

```
wlans-name <WLAN-Service-name>
```

Parameters

<WLAN-Service-name>	Specifies the name of the .WLAN Service to associate with this VNS.

Examples

This example changes the associated WLAN Service to wlan4 for the VNS named VNS1.

```
EWC.enterasys.com:vnsmode:VNS1# wlans-name wlan4
EWC.enterasys.com:vnsmode:VNS1# apply
```

Note: After you run the **wlans-name** command, you must run the **apply** command to implement the changes.

18.8.9 show

Use the **show** command in the **vnsmode:<named-VNS>** context to display information about the current VNS.

Syntax

```
show
```

Parameters

None.

Examples

This example displays information about the current VNS named VNS1.

```
EWC.enterasys.com:vnsmode:VNS1# show
WLANS service: wlan4
Non-authenticated: p4
Authenticated: same as non-authenticated
Restrict available policy set: disable
Enable status: enable
Synchronize: enable
Name: VNS1
```

19

wlans Commands

This section describes commands used to define and configure WLAN services for the network. These commands are located in the **wlans** context of the CLI. Execute the **wlans** command at the root level to enter wlans context.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

Note: The **wlans** context was introduced with V7R0.

The following commands are available in the **wlans** context:

- clients — See clients for commands in the **wlan:clients** context.
- create
- delete
- remote-ssid
- show
- <WLAN-service-name> — See <WLAN-service-name> for commands in the **wlan:<WLAN-service-name>** context.

19.1 clients

The **clients** context provides commands which are used to configure guest access features on the Enterasys Wireless Controller. Switch to the **clients** context from the **wlans** context to access the following commands on the Enterasys Wireless Controller.

Note: A guest portal WLAN service must be created on this controller before the **clients** context command and the context's associated commands are available. For more on creating a guest portal WLAN service, see “mode” on page 19-32.

The following commands are available in the **wlan:clients** context.

- client
- descr
- enable
- endofday
- export_clients

- import_clients
- startofday

19.1.1 client

Use the **client** command to configure the guest portal client access account.

Syntax

```
[no] client <id> <name> <passwd> <acct_start> <account_lifetime>
<session_lifetime>
```

Parameters

<id>	Specifies the ID of the guest access account and must begin with the string “Guest-”
<name>	Specifies the name of the client
<passwd>	Specifies the password used by the client
<acct_start>	Specifies the activation start time of the client account (in the form YYYY-MM-DD HH:MM:SS)
<account_lifetime>	Specifies the amount of time the client account will remain viable
<session_lifetime>	Specifies the amount of time the client session will remain viable

Examples

The following example configures a client guest access account named “Lobby.”:

```
EWC.enterasys.com:wlans:clients# client Guest-lobby Lobby 1234abcd 2009-12-01
12:00:00 12 12
EWC.enterasys.com:wlans:clients# show
Guest-lobby    Lobby   1234abcd      2009-12-01 12:00:00    12     12    00:00
00:00   disabled
```

19.1.2 descr

Use the **descr** command to add a description to the specified guest portal client access account.

Syntax

```
descr <id> <descriptive_text>
```

Parameters

<id>	Specifies the ID of the guest access account and must begin with the string “Guest-”
<descriptive_text>	Specifies the description for the guest client

Examples

The following example sets a description for the client guest access account with ID "Guest-lobby":

```
EWC.enterasys.com:EWC.enterasys.com:wlans:clients# descr Guest-lobby The lobby guest client account.
EWC.enterasys.com:wlans:clients# show descr
Guest-lobby    Lobby   1234abcd       2009-12-01 12:00:00    12      12     The lobby guest client account.        00:00   00:00   disabled
```

The following example clears the description for the client guest access account with ID "Guest-lobby"

```
EWC.enterasys.com:wlans:clients# descr Guest-lobby
EWC.enterasys.com:wlans:clients# show
Guest-lobby    Lobby   1234abcd      2009-12-01 12:00:00   12      12
00:00   00:00   disabled
```

19.1.3 enable

Use the **enable** command to enable or disable the guest portal access account

Syntax

```
[no] enable <id>
```

Parameters

<id>	Specifies the ID of the guest access account and must begin with the string "Guest-"

Examples

The following example enables the guest access account:

```
EWC.enterasys.com:wlans:clients# enable Guest-lobby
EWC.enterasys.com:wlans:clients# show
Guest-lobby    Lobby   1234abcd      2009-12-01 12:00:00   12      12
00:00   08:00   enabled
```

The following example disables the guest access account:

```
EWC.enterasys.com:wlans:clients# no enable Guest-lobby
EWC.enterasys.com:wlans:clients# show
Guest-lobby    Lobby   1234abcd      2009-12-01 12:00:00   12      12
00:00   08:00   disabled
```

19.1.4 endofday

Use the **endofday** command to configure the duration of the guest portal access account.

Syntax

```
[no] endofday <id> <HH:MM>
```

Parameters

<id>	Specifies the ID of the guest access account and must begin with the string "Guest-"
<HH:MM>	Specifies the duration of the guest client in a <HH:MM> hours and minutes format

Examples

The following example sets the duration of the guest access account to 8 hours:

```
EWC.enterasys.com:wlans:clients# endofday Guest-lobby 08:00
EWC.enterasys.com:wlans:clients# show
Guest-lobby    Lobby   1234abcd      2009-12-01 12:00:00   12      12
00:00   08:00   disabled
```

19.1.5 export_clients

Use the **export_clients** command to export all current client information from the system to a file.

Syntax

```
export_clients <server> <user> <dir> <file>
```

Parameters

<server>	Specifies the IP address of an FTP server to export the file to
<user>	Specifies the username with which to login in to the FTP server
<dir>	Specifies the directory path containing the clients export file
<file>	Specifies the clients export file name

Examples

The following example exports all current client information from the system to a file named clients_export:

```
EWC.enterasys.com:wlans:clients# export_clients 192.168.4.1 admin /support
clients_export_file
Please input password:
Attempting to upload file using ncftp ...
```

19.1.6 import_clients

Use the **import_clients** command to import client information into the system from a file.

Syntax

```
import_clients <server> <user> <dir> <file>
```

Parameters

<server>	Specifies the IP address of an FTP server to import the file from

<user>	Specifies the username with which to login in to the FTP server
<dir>	Specifies the directory path containing the clients import file
<file>	Specifies the clients import file name

Examples

The following example imports the previously exported file created by the export_clients command:

```
EWC.enterasys.com:wlans:clients# import_clients 192.168.4.1 admin /support
clients_export_file
Please input password:
Attempting to download file...
```

19.1.7 startofday

Use the **startofday** command to configure the time for start of day for the guest portal access account.

Syntax

```
[no] startofday <id> <HH:MM>
```

Parameters

<id>	Specifies the ID of the guest access account and must begin with the string "Guest-"
<HH:MM>	Specifies the account activation time. The default is 00:00.

Examples

The following example sets the account activation time of the guest access account to 07:00 hours:

```
EWC.enterasys.com:wlans:clients# startofday Guest-lobby 07:00
EWC.enterasys.com:wlans:clients# show
Guest-lobby    Lobby   1234abcd      2009-12-01 12:00:00   12      12
07:00   07:00   disabled
```

19.2 create

Use the **create** command to create a WLAN service configuration. The **create** command is accessible from the **wlans** context of the CLI.

Syntax

```
create <WLANS-name> mode (mesh|wds|std|3pap|remote) ssid <ssid-string>
```

Parameters

<WLANS-name>	Specifies the name of the WLAN service
mode (mesh|wds|std|3pap|remote)	Specifies the mode of the WLAN service

ssid <ssid-string>	Specifies the SSID of the WLAN service

Examples

The following example creates and then displays the details of a WLAN service configuration named test-wlan in WDS mode with an SSID of "test":

```
EWC.enterasys.com:wlans# create test-wlan mode wds ssid test
EWC.enterasys.com:wlans# show test-wlan
Service type: wds
Pre-shared Key:
Name: test-wlan
Enable status: enable
Pre-shared Key:
SSID: test
```

19.3 delete

Use the **delete** command to delete a WLAN service configuration. The **delete** command is accessible from the **wlans** context of the CLI.

Syntax

```
delete <WLANS-name>
```

Parameters

<WLANS-name>	Specifies the name of the WLAN service to delete

Examples

The following example deletes the WLAN service named test-wlan:

```
EWC.enterasys.com:wlans# delete test-wlan
```

19.4 remote-ssid

Use the **remote-ssid** command to display the available remote SSIDs within the HiPath Wireless Controller's mobility domain.

Syntax

```
remote-ssid
```

Parameters

None.

Usage

The **remote-ssid** command reports the remote SSIDs only if the **remoteable** command is set to **enable**. For more information, see "remoteable" on page 19-54.

Examples

The following example displays the currently available remote SSIDs.

```
EWC.enterasys.com:wlans# remote-ssid
There is no remotable SSID in the mobility domain.
```

19.5 show

Use the show command from the **wlans** context to display WLAN service configuration information.

Syntax

show [<WLANS-name>]

Parameters

<WLANS-name>	Specifies to display information about the specific WLAN service

Examples

The following example displays a list of all WLAN service configuration information:

```
EWC.enterasys.com:wlans# show

Name         Service Type  Enabled   SSID            Privacy  Auth Mode    Radio Mode

test         std           disabled  test            wep      disabled     off
gp1          std           enabled   gp1             none     guestportal  off
test_remote  remote        enabled   testremotessid  none     disabled     off
```

The following example displays configuration information for the WLAN service named "Lab12-open":

```
EWC.enterasys.com:wlans# show Lab12-open
Service type: std
Name: Lab12-open
Synchronize: enable
Enable status: enable
Wireless AP Services:
Wireless AP: 0500000000000000
Wireless AP: 1000000000000000
Wireless AP: 5555555555555555  (foreign)
Wireless AP: ap 3262  (foreign)
Wireless AP: z101 AP2610 m  (foreign)
Wireless AP: z102 AP2610-1 m  (foreign)
Wireless AP: z103 AP2620 m  (foreign)
Wireless AP: z104 AP2620-1 m  (foreign)
Wireless AP: z105 AP2630 m  (foreign)
```

```
Wireless AP: z106 AP2630-1 m  (foreign)
Wireless AP: z201 AP3610 m  (foreign)
Wireless AP: z202 AP3610-1 m  (foreign)
Wireless AP: z301 AP2650 m  (foreign)
Wireless AP: z302 AP2650-1 m  (foreign)
Wireless AP: z901 APW788 m  (foreign)
SSID: Lab12-open
pre-authentication timeout(minutes): 5
post-authentication timeout(minutes): 30
session timeout(minutes): 0
Block MU to MU traffic: disable
```

19.6 <WLAN-service-name>

The **<WLAN-service-name>** command, where <WLAN-service-name> is the name of a given WLAN service, moves you into the **wlan:<WLAN-service-name>** context, which contains commands to configure the settings of the specified individual WLAN service.

The following commands are available in the **wlan:<WLAN-service-name>** context. Different commands are available depending on the type of WLAN server being configured.

- 3pap
- aplist
- aplist-wds (WDS)
- aplist-wds (Mesh)
- auth — See auth for commands in the **wlan:<WLAN-service-name>:auth** context.
- default-topology
- direct-client-traffic
- name
- priv — See priv for commands in the **wlan:<WLAN-service-name>:priv** context.
- psk
- qos-policy — See qos-policy for commands in the **wlan:<WLAN-service-name>:qos-policy** context.
- remoteable
- rf — See rf for commands in the **wlan:<WLAN-service-name>:rf** context.
- show
- ssid
- status
- sync
- timeout-post
- timeout-pre
- timeout-session

19.6.1 3pap

Use the **3pap** command to add a third party AP to the WLAN service configuration. Use the [no] form of the command to remove a third party AP from the WLAN service configuration. The **3pap** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI when the WLAN service type is 3PAP.

Syntax

```
[no] 3pap <A.B.C.D> <HH:HH:HH:HH:HH:HH>
```

Parameters

<A.B.C.D>	Specifies the IPv4 address of the third party AP to add to or remove from the WLAN service
<HH:HH:HH:HH:HH:HH>	Specifies the MAC address of the third party AP to add to or remove from the WLAN service

Usage

This command is only available when the WLAN service type is third party AP (3pap).

Examples

The following example adds a third party AP by IP and MAC address to the WLAN service named “3pap-test”:

```
EWC.enterasys.com:wlans:3pap-test# 3pap 1.2.3.4 11:22:33:44:55:66
EWC.enterasys.com:wlans:test# apply
```

Note: After you run the **3pap** command, you must run the **apply** command to implement the changes.

19.6.2 aplist

Use the **aplist** command to add or remove an AP to or from the WLAN service configuration. The **aplist** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI when the WLAN service type is standard.

Syntax

```
[no] aplist <ap-name> radio1|radio2|both
```

Parameters

<ap-name>	Specifies the name of the AP to add or remove from the WLAN service. The no form of the command removes the AP
radio1|radio2|both	Specifies to use radio1, radio2, or both with the WLAN service

Usage

This command is only available when the WLAN service type is STD.

Examples

The following example adds an AP by serial number to the WLAN service named "test" and then displays the list of Wireless APs:

```
EWC.enterasys.com:wlans:test# aplist 0500000000000000 both
EWC.enterasys.com:wlans:test# apply
EWC.enterasys.com:wlans:test# show aplist
Wireless AP Services:
Wireless AP: 0500000000000000 both
```

Note: After you run the **aplist** command, you must run the **apply** command to implement the changes.

19.6.3 aplist-wds (WDS)

Use the **aplist-wds** command to add or remove an AP to or from a WDS type WLAN service configuration. The **aplist-wds** command is accessible from the **wlans:<WLAN-service-name>** context of the CLI when the WLAN service type is WDS.

Refer to "19.6.4 aplist-wds (Mesh)" on page 19-11 for information about using the command to configure a dynamic mesh WLAN service.

Use this command to configure the following:

- Role on radio 1
- Role on radio 2
- Preferred parent
- Backup parent
- Work group bridging

Syntax

```
aplist-wds <ap-name> ((radio1 <none|child|parent|both> radio2
<none|child|parent|both>)|(both <none|child|parent|both>)) [pref-parent <ap-name
| Any-Parent>] [backup-parent <ap-name | Any-Parent>] [wkgbridge <on|off>]
no aplist-wds <ap-name> radio1|radio2|both
```

Parameters

radio1 <none | child | parent | both>	Specifies the AP's role on Radio1
radio2 < none | child | parent | both>	Specifies the AP's role on Radio2
both < none | child | parent | both>	Specifies the AP's role on both radios
pref-parent <ap-name | Any Parent>	Specifies the AP's parent
backup-parent <ap-name | Any Parent>	Specifies the AP's backup parent
wkgbridge <off | on>	Configures the work group bridging

Usage

This command is only available when the WLAN service type is WDS.

Examples

The following example reflects the following:

- AP Lancaster is serving as a child of AP Aruba on radio **radio1**
- AP Auberon is the backup parent of AP Lancaster
- Work group bridging is switched off

```
EWC.enterasys.com:wlans:shopfloor_WDS_wlan# aplist-wds Lancaster radio1 child
radio2 parent pref-parent Aruba backup-parent Auberon wkgbridge off
EWC.enterasys.com:wlans:shopfloor_WDS_wlan# apply
```

Note: After you run the **aplist-wds** command, you must run the **apply** command to implement the changes.

19.6.4 aplist-wds (Mesh)

Use the **aplist-wds** command to add an AP to a dynamic mesh type WLAN service configuration. The **aplist-wds** command is accessible from the **wlans:<WLAN-service-name>** context of the CLI when the WLAN service type is mesh.

Refer to "19.6.3 aplist-wds (WDS)" on page 19-10 for information about using the command to configure a WDS type of WLAN service.

Syntax

```
aplist-wds <ap-name> (none|portal|mesh) [wkgbridge (on|off)] [radio1|radio2]
```

Parameters

ap-name	Name of the AP being assigned to the WLAN service.
none|portal|mesh	**none** = default, not assigned to the WLAN service. **portal** = the AP is a mesh portal (equivalent to parent in static mesh WLANs). **mesh** = the AP is a mesh AP.
wkgbridge (on|off)	Configures the work group bridging
radio1|radio2	For a dual-band radio AP, if more than one available radio matches the backhaul radio settings, select one of the radios for backhaul.

Usage

An AP can be assigned to either a static mesh/WDS WLAN service or a dynamic mesh WLAN service, but not to both types of mesh service at the same time.

On dual-band APs, if only one radio matches the backhaul radio band, selecting a radio is optional. If a radio is selected but it is the wrong one, the system will print an error message.

If more than one radio matches the backhaul radio band, then selecting a radio is mandatory and an error message will print if no radio is selected.

Examples

The following example adds the AP named lab-ap1 as a mesh portal with work group bridging on for dynamic mesh WLAN mesh1-wlan.

```
EWC.enterasys.com:wlans:mesh1-wlan# aplist-wds lab-ap1 portal wkgbridge on
```

19.6.5 auth

The **auth** command moves you into the authentication context, **wlans:<WLAN-service-name>:auth**, for the configuration of authentication settings for the WLAN service being configured. The WLANS auth context supports the following authentication types:

- MAC
- 802.1X mode
- Captive Portal Authentication modes: internal, external, guest portal, and guest splash

When you first enter the auth context, MAC, 802.1x and Captive Portal Authentication modes default to disabled. MAC authentication can be configured in any authentication mode. The availability of non-MAC authentication commands depends upon the mode you are currently in. The Usage section for each authentication command specifies mode information for that command. See "mode" on page 19-32 for further information on setting the authentication mode.

The following commands are available in the **wlans:<WLAN-service-name>:auth** context.

- aaa-redir
- auth-ap
- auth-egress
- auth-ingress
- auth-policy
- auth-ssid
- auth-topology
- auth-vns
- captiveportal — See captiveportal for commands in the **wlans:<WLAN-service-name>:captiveportal** context.
- cdr
- config
- interim
- mac
- mac-auto-authenticate
- mac-allow-unauthorized
- mac-roam
- mode
- move
- nasid
- nasip
- password

- protocol
- remove
- show

19.6.5.1 aaa-redir

Use the **aaa-redir** command to enable or disable AAA redirect.

Syntax

```
aaa-redir enable | disable
```

Parameters

enable | disable	Specify to enable or disable AAA redirect

Usage

The **8021x** authentication mode must be set for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables AAA redirect:

```
EWC.enterasys.com:wlans:cnl-AAA:auth# aaa-redir enable
EWC.enterasys.com:wlans:cnl-AAA:auth# apply
```

Note: After you run the **aaa-redir** command, you must run the **apply** command to implement the changes.

19.6.5.2 auth-ap

Use the **auth-ap** command to include AP Identification in the message to the RADIUS server. The **auth-ap** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
auth-ap enable | disable
```

Parameters

enable | disable	Specifies to enable or disable the inclusion of AP Identification information in messages to the RADIUS server

Usage

The **auth-ap** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables the inclusion of AP Identification information in messages to the RADIUS server:

```
EWC.enterasys.com:wlans:test:auth# auth-ap enable
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show auth-ap
AP as VSA attribute: enable
```

Note: After you run the **auth-ap** command, you must run the **apply** command to implement the changes.

19.6.5.3 auth-egress

Use the **auth-egress** command to include egress rate control information in the message to the RADIUS server. The **auth-egress** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
auth-egress enable | disable
```

Parameters

enable | disable	Specifies to enable or disable the inclusion of egress rate control information in messages to the RADIUS server

Usage

The **auth-egress** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables the inclusion of egress rate control information in messages to the RADIUS server:

```
EWC.enterasys.com:wlans:test:auth# auth-egress enable
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show auth-egress
Egress rate control as VSA attribute: enable
```

Note: After you run this command, you must run the **apply** command to implement the changes.

19.6.5.4 auth-ingress

Use the **auth-ingress** command to include ingress rate control information in the message to the RADIUS server. The **auth-ingress** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
auth-ingress enable | disable
```

Parameters

enable | disable	Specifies to enable or disable the inclusion of ingress rate control information in messages to the RADIUS server

Usage

The **auth-ingress** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables the inclusion of ingress rate control information in messages to the RADIUS server:

```
EWC.enterasys.com:wlans:test:auth# auth-ingress enable
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show auth-ingress
Ingress as VSA attribute: enable
```

Note: After you run this command, you must run the **apply** command to implement the changes.

19.6.5.5 auth-policy

Use the **auth-policy** command to include policy information in the message to the RADIUS server. The **auth-policy** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
auth-policy enable | disable
```

Parameters

enable | disable	Specifies to enable or disable the inclusion of policy information in messages to the RADIUS server

Usage

The **auth-policy** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables the inclusion of policy information in the message to the RADIUS server:

```
EWC.enterasys.com:wlans:test:auth# auth-policy enable
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show auth-policy
Policy as VSA attribute: enable
```

Note: After you run this command, you must run the **apply** command to implement the changes.

19.6.5.6 auth-ssid

Use the **auth-ssid** command to include SSID information in the message to the RADIUS server. The **auth-ssid** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
auth-ssid enable | disable
```

Parameters

enable | disable	Specifies to enable or disable the inclusion of SSID information in messages to the RADIUS server

Usage

The **auth-ssid** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables the inclusion of SSID information in messages to the RADIUS server:

```
EWC.enterasys.com:wlans:test:auth# auth-ssid enable
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show auth-ssid
SSID as VSA attribute: enable
```

Note: After you run this command, you must run the **apply** command to implement the changes.

19.6.5.7 auth-topology

Use the **auth-topology** command to include topology information in the message to the RADIUS server. The **auth-topology** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
auth-topology enable | disable
```

Parameters

enable | disable	Specifies to enable or disable the inclusion of Topology information in messages to the RADIUS server

Usage

The **auth-topology** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables the inclusion of Topology information in messages to the RADIUS server:

```
EWC.enterasys.com:wlans:test:auth# auth-topology enable
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show auth-topology
Topology as VSA attribute: enable
```

Note: After you run this command, you must run the **apply** command to implement the changes.

19.6.5.8 auth-vns

Use the **auth-vns** command to include VNS information in the message to the RADIUS server. The **auth-vns** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
auth-vns enable | disable
```

Parameters

enable | disable	Specifies to enable or disable the inclusion of VNS information in messages to the RADIUS server

Usage

The **auth-vns** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables the inclusion of VNS information in messages to the RADIUS server:

```
EWC.enterasys.com:wlans:test:auth# auth-vns enable
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show auth-vns
VNS as VSA attribute: enable
```

Note: After you run this command, you must run the **apply** command to implement the changes.

19.6.5.9 captiveportal

The Enterasys Wireless Controller can use Captive Portal authentication for Service Set Identifier (SSID) network assignments. The Captive Portal is a browser-based authentication mechanism that forces unauthenticated users to a web page.

The **captiveportal** command moves you to context **wlan:<WLAN-service-name>:auth:captiveportal**, which contains commands used to configure Captive Portal support.

Note: In V7.0, the new **wlan:<WLAN-service-name>:auth:mode** command (mode) determines which commands are available in the captiveportal context.

The following commands are available in the **wlan:<WLAN-service-name>:auth:captiveportal** context.

- add-ip-port
- copy-cpfile
- cp-ssl
- custom
- extcpip
- extredir
- extsecret
- fqdn
- guestportalacctlifetime
- guestportalprefix
- maxsessionlifetime
- minpasswdlength
- redirect
- send-login
- set-acct-lifetime
- tos-override

19.6.5.9.1 add-ip-port

Use this command enable or disable the ability to add a controller IP address and port to the redirection URL. The add-ip-port command is available in the **wlan:<WLAN-service-name>:auth:captiveportal** context for external captive portal mode only.

Syntax

```
add-ip-port enable | disable
```

Parameters

enable	Enable adding a controller IP address and port to the redirection URL.
disable	Disable adding a controller IP address and port to the redirection URL. This is the default.

19.6.5.9.2 copy-cpfile

Use this command to download a zip file containing customized web pages. The **copy-cpfile** command is available from the **wlan:<WLAN-service-name>:auth:captiveportal** context.

Syntax

```
copy-cpfile  <scp|ftp>  <server> <user> <password> <dir> <file>
```

Parameters

scp | **ftp**	Specifies whether to use FTP or SCP to download the file.
server	The IP address of the FTP or SCP server.
user	The user name to log in to the server.
password	The password for file transfer protocol.
dir	The directory on the server where the file is located.
file	The name of the file containing the web pages.

Examples

This example uses FTP to copy the file “cpcustom.zip” located in the /tmp directory on FTP server 192.168.3.10, using log in credentials “root” and “mypasswd.”

```
EWC.enterasys.com:wlans:Lab126-12-Int-CP:auth:captiveportal# copy-cpfile ftp
192.168.3.10 root mypasswd /tmp cpcustom.zip
```

19.6.5.9.3 cp-ssl

Use the **cp-ssl** command to enable or disable HTTPS support on a WLAN service configured for external authentication. The **cp-ssl** command is available only if **mode** is set to **external**. For more information about the **mode** command, see “mode” on page 19-32.

Syntax

```
cp-ssl enable|disable
```

Parameters

enable	Enable HTTPS support on the WLAN service configured for external authentication.

disable	Disable HTTPS support on the WLAN service configured for external authentication.

Usage

By default, HTTPS support is disabled.

Examples

The following example enables HTTPS support on the WLAN service.

```
EWC.enterasys.com:wlans:external_wlan:auth:captiveportal# cp-ssl enable
EWC.enterasys.com:wlans:external_wlan:auth:captiveportal# apply
```

19.6.5.9.4 custom

Use the **custom** command, within context **wlan:<WLAN-service-name>:auth:captiveportal,** to configure communications options for custom captive portal settings.

Syntax

```
custom local | web
```

Parameters

local	Sets captive portal communications options to local
web	Sets captive portal communications options to web

Usage

If customized captive portal content was previously downloaded to the controller using the **copy-custom** command, **custom** can only be successfully set to local. The internal or splash authentication mode must be set for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example sets the captive portal communications options to web:

```
EWC.enterasys.com:wlans:new-wlans:auth:captiveportal# custom web
EWC.enterasys.com:wlans:new-wlans:auth:captiveportal# apply
```

Note: After you run the **custom** command, you must run the **apply** command to implement the changes.

19.6.5.9.5 extcpip

Use the **extcpip** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to specify the interface and the server access port on the Enterasys Wireless Controller for communication with an external Enterasys Wireless Controller.

Syntax

```
extcpip (esa<X>|eth0):<port>
```

For a Enterasys Wireless Controller C20N the syntax is:

```
extcpip (PC.<X>|eth0):<port>
```

For a Enterasys Wireless Controller C4110 the syntax is:

```
extcpip port<X>:<port>
```

Parameters

PC.<X>	Indicates that a physical data port will be used, where X is an identification number between 0 and 3.
esa<X>	Indicates that a physical data port will be used, where X is an identification number between 0 and 3
port<X>	Indicates that a physical data port will be used, where X is an identification number between 1 and 4
eth0	Indicates that the management interface will be used
<port>	Specifies the port number within the range: 32768 - 65535

Usage

Either the external authentication mode or 802.1x with aaa-redir must be set for this command to be available. For more information, see “mode” on page 19-32.

Examples

The following example specifies the interface and port of an external Enterasys Wireless Controller:

```
EWC.enterasys.com:wlans:CNL-7-CP:auth:captiveportal# extcpip esa0:32850
EWC.enterasys.com:wlans:CNL-7-CP:auth:captiveportal# apply
```

Note: After you run the **extcpip** command, you must run the **apply** command to implement the changes.

19.6.5.9.6 extredir

Use the **extredir** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to specify the External Redirection URL.

Syntax

```
extredir <value_string> | none
```

Parameters

<value_string>	Specifies a URL beginning with http://
none	Specifies that no external redirection URL is configured

Usage

The external authentication mode must be set for this command to be available. For more information, see “mode” on page 19-32.

Examples

The following example specifies an External Redirection URL:

```
EWC.enterasys.com:wlans:CNL-7-CP:auth:captiveportal# extredir http://
192.168.4.89:80
EWC.enterasys.com:wlans:CNL-7-CP:auth:captiveportal# apply
```

Note: After you run the **extredir** command, you must run the **apply** command to implement the changes.

19.6.5.9.7 extsecret

Use the **extsecret** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to define the Shared Secret password common to both the Enterasys Wireless Controller and the external web server.

Syntax

```
extsecret <value_string> | none
```

Parameters

<value_string>	Specifies a password
none	Specifies that no password is configured

Usage

The external authentication mode must be set for this command to be available. For more information, see “mode” on page 19-32.

Examples

The following example creates a Shared Secret password:

```
EWC.enterasys.com:wlans:CNL-7-CP:auth:captiveportal# extsecret 5eCretH4nD5h4k3
EWC.enterasys.com:wlans:CNL-7-CP:auth:captiveportal# apply
```

Note: After you run the **extsecret** command, you must run the **apply** command to implement the changes.

19.6.5.9.8 fqdn

Use the **fqdn** command, within context **wlan:<WLAN-service-name>:auth:captiveportal,** to replace the Gateway IP address with a Fully Qualified Domain Name (FQDN).

Syntax

```
fqdn <value_string> | none
```

Parameters

<value_string>	Specifies a domain name
none	Specifies that the Gateway IP address is not replaced with a FQDN

Usage

The guestportal, internal, or splash authentication mode must be set for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example replaces the Gateway IP address with a domain name:

```
EWC.enterasys.com:vnsmode:CNL-7-CP:auth:captiveportal# fqdn cp.siemens.com
EWC.enterasys.com:vnsmode:CNL-7-CP:auth:captiveportal# apply
```

Note: After you run the **fqdn** command, you must run the **apply** command to implement the changes.

19.6.5.9.9 guestportalacctlifetime

Use the **guestportalacctlifetime** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to configure the lifetime for the guest portal access account, in days.

Syntax

```
[no] guestportalacctlifetime <days>
```

Parameters

<days>	Specifies the number of days the account remains valid

Usage

The guestportal authentication mode must be set for this command to be available. For more information, see "mode" on page 19-40.

Examples

The following example sets the guest portal account lifetime to one day:

```
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# guestportalacctlifetime 1
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# apply
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# show guestportalacctlifetime
guestportalacctlifetime 1
```

Note: After you run the **guestportalacctlifetime** command, you must run the **apply** command to implement the changes.

19.6.5.9.10 guestportalprefix

Use the **guestportalprefix** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to configure the user ID prefix for the guest portal access account.

Syntax

```
guestportalprefix <prefix>
```

Parameters

<prefix>	Specifies the maximum number of hours for the session time of the guestportal access account

Usage

The guestportal authentication mode must be set for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example sets the guest portal prefix to the string "TEST":

```
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# guestportalprefix TEST
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# apply
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# show guestportalprefix
guestportalprefix        TEST
```

Note: After you run the **guestportalprefix** command, you must run the **apply** command to implement the changes.

19.6.5.9.11 maxsessionlifetime

Use the **maxsessionlifetime** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to configure the maximum session lifetime for the guest portal access account, in hours.

Syntax

```
[no] maxsessionlifetime <hours>
```

Parameters

<hours>	Specifies the maximum number of hours for the session time of the guestportal access account

Usage

The guestportal authentication mode must be set for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example sets the maximum session lifetime for the guest portal account to one hour:

```
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# maxsessionlifetime 1
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# apply
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# show maxsessionlifetime
maxsessionlifetime      1
```

Note: After you run the **maxsessionlifetime** command, you must run the **apply** command to implement the changes.

19.6.5.9.12 minpasswdlength

Use the **minpasswdlength** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to set the minimum acceptable character length for the password for the guest portal access account.

Syntax

```
minpasswdlength <length>
```

Parameters

<length>	Specifies the minimum acceptable character length for the guest portal access account password

Usage

The guestportal authentication mode must be set for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example sets the minimum length for the guest portal access account password to 12 characters:

```
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# minpasswdlength 12
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# apply
EWC.enterasys.com:wlans:CNL-CP:auth:captiveportal# show minpasswdlength
minpasswdlength 12
```

Note: After you run the **minpasswdlength** command, you must run the **apply** command to implement the changes.

19.6.5.9.13 redirect

Use the **redirect** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to specify the Default Redirection URL.

Syntax

```
redirect <value_string> | none
```

Parameters

<value_string>	Specifies a URL beginning with http://
none	Specifies that no Default Redirection URL is configured

Usage

The guestportal, internal or splash authentication mode must be set for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example specifies the internal network URL to redirect connecting users to:

```
EWC.enterasys.com:vnsmode:CNL-7-CP:auth:captiveportal# redirect http://
192.168.1.38
EWC.enterasys.com:vnsmode:CNL-7-CP:auth:captiveportal# apply
```

Note: After you run the **redirect** command, you must run the **apply** command to implement the changes.

19.6.5.9.14 send-login

Use this command to specify the type of captive portal redirection URL for successful logins. The **send-login** command is available from the **wlan:<WLAN-service-name>:auth:captiveportal** context.

Syntax

```
send-login original-dest | cp-session | custom
```

Parameters

original-dest	Use the original destination value configured by the Wireless Assistant GUI.
cp-session	Use the captive portal session page value configured by the Wireless Assistant GUI.
custom	Use the custom specific URL value configured by the Wireless Assistant GUI.

Examples

This example specifies that the type of successful login redirection URL is custom.

```
EWC.enterasys.com:wlans:Lab126-12-Int-CP:auth:captiveportal# send-login custom
```

19.6.5.9.15 set-acct-lifetime

Use this command to enable or disable the ability of the Guest Administrator to set account lifetimes. The **set-acct-lifetime** command is available from the **wlan:<WLAN-service-name>:auth:captiveportal** context for guest portal mode only.

Syntax

```
set-acct-lifetime enable | disable
```

Parameters

enable	Enables the ability of the Guest Administrator to set account lifetimes.
disable	Disables the ability of the Guest Administrator to set account lifetimes. Disabled is the default.

Usage

If this feature is enabled, after the guest administrator logs in, the “Account Lifetime” field will be enabled when updating accounts or adding new guest accounts.

Examples

This example enables the ability of the Guest Administrator to set account lifetimes.

```
EWC.enterasys.com:wlans:Lab126-12-GuestP:auth:captiveportal# set-acct-lifetime
enable
```

19.6.5.9.16 tos-override

Use the **tos-override** command, within context **wlan:<WLAN-service-name>:auth:captiveportal**, to enable or disable external portal integration with Policy Manager (NAC). This command is available when the named WLAN service is in "external" mode.

Syntax

```
tos-override (enable tos <HH>) | disable
```

Parameters

enable tos	Enables ToS override
<HH>	Specifies a hexidecimal value for ToS override. For the NAC integration, this should be 40 (0x40)
disable	Disables ToS override

Usage

This command is used to configure an external portal integration with NAC where HTTP traffic for non authenticated users is tagged with a ToS override value. To integrate with NAC, you must use this command to set the hexidecimal ToS override value on the controller to 0x40.

The external authentication mode must be set for this command to be available. For more information, see "mode" on page 19-32.

Examples

The following example enables ToS override with the hex value required for NAC integration (0x40):

```
EWC.enterasys.com:wlans:new-wlans:auth:captiveportal# tos-override enable tos 40
EWC.enterasys.com:wlans:new-wlans:auth:captiveportal# apply
EWC.enterasys.com:wlans:new-wlans:auth:captiveportal# show tos-override
ToS override for NAC Value(Hex):0x40
```

Note: After you run the **tos-override** command, you must run the **apply** command to implement the changes.

19.6.5.10 cdr

Use the **cdr** command to enable or disable the collection of Wireless Controller accounting information. The **cdr** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
cdr enable | disable
```

Parameters

enable | disable	Specifies to enable or disable the collection of Wireless Controller accounting information

Usage

The **cdr** command is available in all authentication modes. For more information, see "mode" on page 19-32.

Examples

The following example enables the collection of Wireless Controller accounting information:

```
EWC.enterasys.com:wlans:test:auth# cdr enable
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show cdr
Collecting accounting information of Wireless Controller: enable
```

Note: After you run the **cdr** command, you must run the **apply** command to implement the changes.

19.6.5.11 config

The **config** command defines RADIUS server settings for the named WLAN service in the current context, overriding default RADIUS server configuration. The **config** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI. Use this command to configure the RADIUS server as an accounting, authentication or MAC authentication server.

Syntax

```
config (<radius> (role acct|auth|mac) [prot CHAP | PAP | MS-CHAP | MS-CHAP2])
```

Parameters

<radius>	Specifies the name of the RADIUS server to configure
role acct|auth|mac	Specifies the role of the RADIUS server as accounting, authentication, or MAC authentication server, respectively.
prot CHAP | PAP | MS-CHAP | MS-CHAP2]	Specifies the Authentication type

Usage

The **config** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For authentication **mode** command information, see "mode" on page 19-32. For **mac** command information, see "mac" on page 19-30.

For third party APs SSIDs, this command is only visible when **mac** is set to enable and only mac authentication is supported.

After executing the **config** command to configure a RADIUS server, you can proceed to configure additional server attributes such as NAS ID and NAS IP address. When you are finished

configuring RADIUS server attributes, use the **exit** command to return to the **wlans:<WLAN-service-name>** context.

Examples

The following example configures the RADIUS server "radius1" as an authentication server:

```
EWC.enterasys.com:wlans:cnl-AAA:auth# config radius1 role auth prot PAP
EWC.enterasys.com:wlans:cnl-AAA:auth# show
Current selected Radius server radius1 role auth

Priority  Name     Role  NAS IP              NAS ID        Auth Type
1         radius1  auth  Use VNS IP address  Use VNS name  PAP

NAS identifier: Use VNS name
NAS IP address: Use VNS IP address
Authentication type: PAP
```

19.6.5.12 config exit

Use the **config exit** command to exit the RADIUS server configuration mode. The **config exit** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
config exit
```

Parameters

None

Usage

Using the **config exit** command from within the RADIUS server configuration command mode exits the **wlans:<WLAN-service-name>:auth** RADIUS server configuration context and places you in the **wlans:<WLAN-service-name>:auth** context.

Examples

The following example exits the RADIUS server configuration command mode:

```
EWC.enterasys.com:wlans:cnl-AAA:auth# config exit
EWC.enterasys.com:wlans:cnl-AAA:auth#
```

19.6.5.13 interim

Use the **interim** command to configure the RADIUS accounting server interim accounting interval. The **interim** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
interim <interim-interval-value>
```

Parameters

<interim-interval-value>	Specify an integer value in minutes for the interim interval. The default value is 30 minutes.

Usage

The **interim** command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For authentication **mode** command information, see "mode" on page 19-32. For **mac** command information, see "mac" on page 19-30.

Examples

The following example sets the interim value to 40 minutes:

```
EWC.enterasys.com:wlans:test:auth# interim 40
```

19.6.5.14 mac

Use the **mac** command to enable or disable MAC based authentication. The **mac** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
mac enable | disable
```

Parameters

enable | disable	Specifies to enable or disable MAC based authentication

Usage

The **mac** command is not available in the guest splash and guest portal authentication modes. For more information, see "mode" on page 19-32.

Examples

The following example enables MAC authentication for the test WLANS:

```
EWC.enterasys.com:wlans:test:auth# mac enable
EWC.enterasys.com:wlans:test:auth# show mac
MAC based authorization: enable
```

19.6.5.15 mac-auto-authenticate

Use the **mac-auto-authenticate** command to automatically authenticate authorized users. The **mac-auto-authenticate** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
mac-auto-authenticate enable | disable
```

Parameters

enable | disable	Specify to enable or disable automatic authentication of authorized users

Usage

The **mac-auto-authenticate** command is available in all authentication modes, if MAC authentication is enabled, using the **mac enable** command. For authentication **mode** command information, see "mode" on page 19-32. For **mac** command information, see "mac" on page 19-30.

Examples

The following example enables automatic authentication of authorized users on the cnl-mac WLANS service:

```
EWC.enterasys.com:wlans:cnl-mac:auth# mac-auto-authenticate enable
EWC.enterasys.com:wlans:cnl-mac:auth# apply
```

Note: After you run the **mac-auto-authenticate** command, you must run the **apply** command to implement the changes.

19.6.5.16 mac-allow-unauthorized

Use the **mac-allow-unauthorized** command to allow the authentication of unauthorized users. The **mac-allow-unauthorized** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
mac-allow-unauthorized enable | disable
```

Parameters

enable | disable	Specify to enable or disable the authentication of unauthorized users on this WLANS service

Usage

The **mac-allow-unauthorized** command is available in all authentication modes, if MAC authentication is enabled, using the **mac enable** command. For authentication **mode** command information, see "mode" on page 19-32. For **mac** command information, see "mac" on page 19-30.

Examples

The following example enables the authentication of unauthorized users for the cnl-mac WLANS service:

```
EWC.enterasys.com:wlans:cnl-mac:auth# mac-allow-unauthorized enable
EWC.enterasys.com:wlans:cnl-mac:auth# apply
```

Note: After you run the **mac-allow-unauthorized** command, you must run the **apply** command to implement the changes.

19.6.5.17 mac-roam

Use the command to enable or disable MAC based authentication on roam. The **mac-roam** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
mac-roam enable | disable
```

Parameters

enable | disable	Specify to enable or disable MAC authentication on roam. Default value: disabled

Usage

The **mac-roam** command is not available in the guest splash and guest portal authentication modes, if MAC authentication is enabled, using the **mac enable** command. For authentication **mode** command information, see "mode" on page 19-32. For **mac** command information, see "mac" on page 19-30.

Examples

The following example enables MAC authentication on roam for the cnl-mac WLAN service:

```
EWC.enterasys.com:wlans:cnl-mac:auth# mac-roam enable
EWC.enterasys.com:wlans:cnl-mac:auth# apply
```

Note: After you run the **mac-roam** command, you must run the **apply** command to implement the changes.

19.6.5.18 mode

Use the **mode** command to configure the authentication mode for the WLAN service. In V7.0 and later the **mode** command determines which authentication commands are available.

The **mode** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
mode disabled | 8021x | internal | external | guestportal | splash
```

Parameters

disabled	Disables authentication modes
8021x	Enters the 802.1x authentication mode
internal	Enters the internal captive portal authentication mode
external	Enters the external captive portal authentication mode
guestportal	Enters the guestportal captive portal authentication mode
splash	Specifies the guest splash captive portal authentication mode

Note: For information on the captive portal context, See "default-topology" on page 19-38.

Examples

The following example sets the authentication mode to external captive portal:

```
EWC.enterasys.com:wlans:test:auth# mode external
EWC.enterasys.com:wlans:test:auth# apply
EWC.enterasys.com:wlans:test:auth# show mode
Authentication mode: external
```

Note: After you run the **mode** command, you must run the **apply** command to implement the changes.

19.6.5.19 move

Use the **move** command, from within the RADIUS server configuration command mode, to change the position of a RADIUS server in the RADIUS server list. The **move** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
move <current-position> <new-position>
```

Parameters

<current-position>	Specifies the current position of the RADIUS server in the RADIUS server list. Valid values are from 1 - 32.
<new-position>	Specifies the new position of the RADIUS server in the RADIUS server list. Valid values are from 1 - 32.

Usage

You must be in RADIUS server configuration mode for the **move** command to be available. Use the **config** command to enter RADIUS server configuration mode. For more information, see "config" on page 19-28.

Examples

The following example moves the RADIUS server in the RADIUS server list position 2 to position 1 in the RADIUS server list:

```
EWC.enterasys.com:wlans:cnl-AAA:auth# move 2 1
EWC.enterasys.com:wlans:cnl-AAA:auth# apply
```

Note: After you run the **move** command, you must run the **apply** command to implement the changes.

19.6.5.20 nasid

Use the **nasid** command to identify the Network Access Server (NAS) to be used with the RADIUS server being configured. The **nasid** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
nasid <string> | vnsname
```

Parameters

<string>	Specify the ID for the NAS
vnsname	Specifies that the VNS name should be used for the NAS ID

Usage

The NAS ID defaults to the VNS name if this command is not used to specify a NAS ID.

You must be in RADIUS server configuration mode for the **nasid** command to be available. Use the **config** command to enter RADIUS server configuration mode. For more information, see "config" on page 19-28.

Examples

The following example sets the NAS ID for this RADIUS server configuration to the VNS name for the cnl-AAA WLANS auth context:

```
EWC.enterasys.com:wlans:cnl-AAA:auth# nasid vnsname
EWC.enterasys.com:wlans:cnl-AAA:auth# apply
EWC.enterasys.com:wlans:cnl-AAA:auth# show nasid
NAS identifier: Use VNS name
```

Note: After you run the **nasid** command, you must run the **apply** command to implement the changes.

19.6.5.21 nasip

Use the **nasip** command to configure the NAS IP address to be used with the RADIUS server being configured. The **nasip** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
nasip <A.B.C.D> | vnsip
```

Parameters

<A.B.C.D>	Specify the NAS IP address
vnsip	Specifies that the VNS IP address should be used for the NAS IP address

Usage

The NAS IP address defaults to the VNS IP address if this command is not used to specify a NAS IP address.

You must be in RADIUS server configuration mode for the **nasip** command to be available. Use the **config** command to enter RADIUS server configuration mode. For more information, see "config" on page 19-28.

Examples

The following example sets the NAS IP address for this RADIUS server configuration to the VNS IP address for the cnl-AAA WLANS auth context:

```
EWC.enterasys.com:wlans:cnl-AAA:auth# nasip vnsip
EWC.enterasys.com:wlans:cnl-AAA:auth# apply
EWC.enterasys.com:wlans:cnl-AAA:auth# show nasip
NAS identifier: Use VNS IP address
```

Note: After you run the **nasip** command, you must run the **apply** command to implement the changes.

19.6.5.22 password

Use the **password** command to specify the MAC authentication password to be used with the RADIUS server being configured. The **password** command is accessible from within the RADIUS server configuration mode from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
password <password>
```

Parameters

<password>	Specify the MAC authentication password

Usage

You must be in RADIUS server configuration mode for the **password** command to be available. Use the **config** command to enter RADIUS server configuration mode. For more information, see "config" on page 19-28.

Examples

The following example sets the MAC authentication password to **techdoc**:

```
EWC.enterasys.com:wlans:cnl-AAA:auth# password techdoc
EWC.enterasys.com:wlans:cnl-AAA:auth# apply
```

Note: After you run the **password** command, you must run the **apply** command to implement the changes.

19.6.5.23 protocol

Use the protocol command to configure the authentication protocol to be used with the RADIUS server being configured. The **protocol** command is accessible from the **wlans:<WLAN-service-name>:auth** context of the CLI.

Syntax

```
protocol CHAP | PAP | MS-CHAP | MS-CHAP2
```

Parameters

CHAP	Configures the Challenge Handshake Authentication Protocol as the authentication protocol
PAP	Configures the Password Authentication Protocol as the authentication protocol
MS-CHAP	`Configures the Windows specific version of CHAP as the authentication protocol`
MS-CHAP2	`Configures the Windows specific version (Version 2) of CHAP as the authentication protocol`

Usage

You must be in RADIUS server configuration mode for the **protocol** command to be available. Use the **config** command to enter RADIUS server configuration mode. For more information, see "config" on page 19-28.

Examples

The following example configures the CHAP protocol as the authentication protocol for this RADIUS server:

```
EWC.enterasys.com:wlans:cnl-AAA:auth# protocol CHAP
EWC.enterasys.com:wlans:cnl-AAA:auth# apply
```

Note: After you run the **protocol** command, you must run the **apply** command to implement the changes.

19.6.5.24 remove

The **remove** command within context **wlan:<WLAN-service-name>:auth** removes the specified RADIUS server from the list of configured RADIUS servers.

Syntax

```
remove <radius>
```

Parameters

<radius>	Specifies the name of the RADIUS server to remove

Examples

The following example removed the RADIUS server "radius1" from the list of RADIUS servers to be used with the "new-wlans" WLAN:

```
EWC.enterasys.com:wlans:new-wlans:auth# remove radius1
```

19.6.5.25 show

Use the **show** command to display the current authentication settings of the specified individual WLAN service. The **show** command is accessible from the **wlan:<WLAN-service-name>:auth** context of the CLI.

Examples

The following example displays the current authentication settings for the WLAN service named Lab126-12-AAA.:

```
EWC.enterasys.com:wlans:Lab126-12-AAA:auth# show
No radius server has been selected

Priority  Name  Role  NAS IP              NAS ID        Auth Type
1         IAS   auth  Use VNS IP address  Use VNS name  EAP
1         IAS   acct  Use VNS IP address  Use VNS name

MAC-based authorization: disable
Authentication mode: 8021x
AP as VSA attribute: enable
SSID as VSA attribute: enable
VNS as VSA attribute: enable
Policy as VSA attribute: enable
Topology as VSA attribute: enable
Ingress rate control as VSA attribute: enable
Egress rate control as VSA attribute: enable
Interim interval (minutes): 0
Collecting accounting information of Wireless Controller: disable
With external: disable
```

19.6.6 backhaul-radio

Use this command to configure the backhaul radio band for a dynamic mesh WLAN service. The **backhaul-radio** command is accessible from the **wlans:<WLAN-service-name>** context of the CLI for dynamic mesh type WLAN services.

Syntax

```
backhaul-radio a|bg
```

Parameters

a	Select the 5 GHz radio band
bg	Select the 2.4 GHz radio band

Usage

After this command has been executed for the dynamic mesh WLAN service being configured, it will no longer be available.

Examples

This example selects the 5 GHz radio band for the dynamic mesh WLAN service named mesh1-wlan.

```
EWC.enterasys.com:wlans:mesh1-wlan# backhaul-radio a
```

19.6.7 default-topology

Use the **default-topology** command to assign an existing B@AC, B@AP, or routed topology as the default topology for the specified WLAN service. You can also use the **default-topology** command to unassign the default topology. The **default-topology** command is accessible from the **wlans:<WLAN-service-name>** context of the CLI.

For information about B@AC, B@AP, and routed topologies, refer to Chapter 21, **topology Commands**.

Syntax

```
default-topology <Default topology name> | none
```

Parameters

Default topology name	Specify default topology to assign to the WLAN service
none	Unassign the default topology from the WLAN service

Examples

The following example assigns the topology FS-REMOTE to the WLAN service.

```
EWC.enterasys.com:wlans:gp1# default-topology FS-REMOTE
```

19.6.8 direct-client-traffic

Use the **direct-client-traffic** command to enable or disable the blocking of direct client to client communication. The **direct-client-traffic** command is accessible from the **wlans:<WLAN-service-name>** context of the CLI.

Syntax

```
direct-client-traffic enable | disable
```

Parameters

enable	Specify to block direct client to client communication
disable	Specify to allow direct client to client communication

Examples

The following example specifies to block direct client to client communication:

```
EWC.enterasys.com:wlans:test# direct-client-traffic enable
EWC.enterasys.com:wlans:test# apply
EWC.enterasys.com:wlans:test# show direct-client-traffic
Block MU to MU traffic: enable
```

Note: After you run the **direct-client-traffic** command, you must run the **apply** command to implement the changes.

19.6.9 interwlan-roaming

Use this command to enable or disable inter-WLAN roaming on this WLAN service. The **interwlan-roaming** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI.

Syntax

```
interwlan-roaming enable|disable
```

Parameters

enable	Enables the inter-WLAN roaming feature for this WLAN service. This is the default setting.
disable	Disables the inter-WLAN roaming feature.

Examples

This example disables inter-WLAN roaming on the WLAN service named test.

```
EWC.enterasys.com:wlans:test# interwlan-roaming disable
```

19.6.10 name

Use the **name** command to modify the name of this WLAN service. The **name** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI when the WLAN service type is STD.

Syntax

```
name <WLAN-service-name>
```

Parameters

<WLAN-service-name>	Specifies the name to use for this WLAN service

Examples

The following example changes the name of the test WLAN serve to “not-test”:

```
EWC.enterasys.com:wlans:test# name not-test
EWC.enterasys.com:wlans:test# apply
EWC.enterasys.com:wlans:test# show name
Name: not-test
```

Note: After you have run the **name** command, you must run the **apply** command to implement the name change.

19.6.11 priv

The **priv** command moves you to the **wlan:<WLAN-service-name>:priv** context, which contains commands to configure the privacy mode of the specified individual WLAN service.

The following commands are available in the **wlan:<WLAN-service-name>:priv** context.

- group-key-ps
- mode
- wep
- wpa-broadcast-rekey
- wpa-v1
- wpa-v2
- wpa-v2-key-mgmt

19.6.11.1 group-key-ps

Use the **group-key-ps** command to enable or disable the group key power save retry. The **group-key-ps** command is available only if the **mode** command is set to wpa-psk. The **group-key-ps** command is accessible from the **wlan:<WLAN-service-name>:priv** context of the CLI when the WLAN service type is STD.

Syntax

```
group-key-ps enable | disable
```

Paramters

enable	Specify to enable the group key power save retry.
disable	Specify to disable the group key power save retry.

Examples

The following example enable the group key power save retry on the WLAN CNL-208-0.

```
EWC.enterasys.com:wlans:CNL-208-0:priv# group-key-ps enable
```

19.6.11.2 mode

Use the **mode** command to set the privacy mode of this WLAN service. The **mode** command is accessible from the **wlan:<WLAN-service-name>:priv** context of the CLI when the WLAN service type is STD.

Syntax

```
mode none | wep | wpa | wpa-psk | dynwep
```

Parameters

none	Disables privacy mode
wep	Specifies the WEP privacy mode
wpa	Specifies the WPA privacy mode
wpa-psk	Specifies the WPA-PSK privacy mode

dynwep	Specifies the dynamic WEP privacy mode

Usage

Once you have set the privacy mode, new commands become available in the **wlan:<WLAN-service-name>:priv** context. For example, setting the privacy mode to wep provides an additional command (wep) that you can use to configure WEP settings.

Examples

The following example changes the privacy mode of the WLAN service named "test" to WPA-PSK:

```
EWC.enterasys.com:wlans:test:priv# mode wpa-psk
EWC.enterasys.com:wlans:test:priv# apply
EWC.enterasys.com:wlans:test:priv# show mode
Privacy mode: wpa-psk
```

Note: After you have run the **mode** command, you must run the **apply** command to implement the name change.

19.6.11.3 wep

Use the **wep** command to configure WEP privacy settings. The **wep** command is accessible from the **wlan:<WLAN-service-name>:priv** context of the CLI.

Syntax

```
wep key-length <64|128|152> ((key <value>) | (pass-phrase <strings>)) [key-idx
(1|2|3|4)]
```

Parameters

key-length <64|128|152>	Specifies the length of the WEP key (64, 128, or 152 bits)
key <value>	Specifies the WEP key as a hex value
pass-phrase <strings>	Specifies the WEP key as a plain text string
key-idx (1|2|3|4)	Specifies the WEP key index

Usage

The wep command is available when the privacy mode is set to wep. For more information, see "mode" on page 19-40.

Examples

The following example sets the WEP key to 64 bits in length with a pass phrase string of "Sl==p":

```
EWC.enterasys.com:wlans:test:priv# wep key-length 64 pass-phrase Sl==p
EWC.enterasys.com:wlans:test:priv# apply
EWC.enterasys.com:wlans:test:priv# show wep
Static Keys(WEP):
    WEP key length: 64
```

```
Input method: input string
WEP string: Sl==p
```

Note: After you have run the **wep** command, you must run the **apply** command to implement the name change.

19.6.11.4 wpa-broadcast-rekey

Use the **wpa-broadcast-rekey** command to configure the re-key interval for group keys. The **wpa-broadcast-rekey** command is accessible from the **wlan:<WLAN-service-name>:priv** context of the CLI.

Syntax

```
wpa-broadcast-rekey none | <30-86400>
```

Parameters

none	Disables the re-key interval for group keys
<30-86400>	Specifies the re-key interval for group keys in seconds

Usage

The **wpa-broadcast-rekey** command is available when the privacy mode is set to wpa or wpa-psk. For more information, see "mode" on page 19-40.

Examples

The following example sets the WPA re-key interval to 300 seconds:

```
EWC.enterasys.com:wlans:test:priv# wpa-broadcast-rekey 300
EWC.enterasys.com:wlans:test:priv# apply
EWC.enterasys.com:wlans:test:priv# show wpa-broadcast-rekey
Broadcast re-key interval (seconds): 300
```

Note: After you have run the **wpa-broadcast-rekey** command, you must run the **apply** command to implement the name change.

19.6.11.5 wpa-v1

Use the **wpa-v1** command to configure the WPA v1 encryption protocol. The **wpa-v1** command is accessible from the **wlan:<WLAN-service-name>:priv** context of the CLI.

Syntax

```
wpa-v1 auto | tkip | none
```

Parameters

auto | tkip | none	Specifies the WPA v1 encryption protocol

Usage

The **wpa-v1** command is available when the privacy mode is set to wpa or wpa-psk. For more information, see "mode" on page 19-40.

Examples

The following example displays the WPA v1 encryption protocol, sets the WPA v1 encryption protocol to TKIP, and displays the setting:

```
EWC.enterasys.com:wlans:test:priv# show wpa-v1
WPA v.1 encryption is not enabled
EWC.enterasys.com:wlans:test:priv# wpa-v1 tkip
EWC.enterasys.com:wlans:test:priv# apply
EWC.enterasys.com:wlans:test:priv# show wpa-v1
WPA v.1 encryption: tkip
```

Note: After you have run the **wpa-v1** command, you must run the **apply** command to implement the name change.

19.6.11.6 wpa-v2

Use the **wpa-v2** command to configure the WPA v2 encryption protocol. The **wpa-v2** command is accessible from the **wlan:<WLAN-service-name>:priv** context of the CLI.

Syntax

```
wpa-v2 auto | aes | none
```

Parameters

auto | aes | none	Specifies the WPA v2 encryption protocol

Usage

The **wpa-v2** command is available when the privacy mode is set to wpa or wpa-psk. For more information, see "mode" on page 19-40.

Examples

The following example displays the WPA v2 encryption protocol, sets the WPA v2 encryption protocol to AES, and displays the setting:

```
EWC.enterasys.com:wlans:test:priv# show wpa-v2
WPA v.2 encryption is not enabled
EWC.enterasys.com:wlans:test:priv# wpa-v2 aes
EWC.enterasys.com:wlans:test:priv# apply
EWC.enterasys.com:wlans:test:priv# show wpa-v2
WPA v.2 encryption: aes
```

Note: After you have run the **wpa-v2** command, you must run the **apply** command to implement the name change.

19.6.11.7 wpa-v2-key-mgmt

Use the **wpa-v2-key-mgmt** command to configure WPA v2 key management options. The **wpa-v2-key-mgmt** command is accessible from the **wlan:<WLAN-service-name>:priv** context of the CLI.

Syntax

```
wpa-v2-key-mgmt none | both | pre-auth | okc
```

Parameters

none | both | pre-auth | okc	Specifies WPA v2 key management from these options, respectively: none, both pre-authorization and Opportunistic Key Caching (OKC), pre-authorization only, or OKC only

Usage

The **wpa-v2-key-mgmt** command is available when the privacy mode is set to wpa. This command is not available when the privacy mode is set to wpa-psk. For more information, see "mode" on page 19-40.

Examples

The following example sets WPA v2 key management to both pre-authorization and Opportunistic Key Caching (OKC):

```
EWC.enterasys.com:wlans:test:priv# wpa-v2-key-mgmt both
EWC.enterasys.com:wlans:test:priv# apply
EWC.enterasys.com:wlans:test:priv# show wpa-v2-key-mgmt
Key Management Options: both
```

Note: After you have run the **wpa-v2-key-mgmt** command, you must run the **apply** command to implement the name change.

19.6.12 psk

Use the **psk** command to configure a pre-shared key in a dynamic mesh or WDS WLAN service. The **psk** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI for a dynamic mesh or WDS WLAN service.

Syntax

```
psk <shared-secret>
```

Parameters

<shared-secret>	Specify a pre-shared key for this dynamic mesh or WDS WLAN service with a key length of between 8 and 63 characters

Usage

After this command has been used to configure the pre-shared key for a WLAN service, it will no longer be avaiable.

Examples

The following example configures the pre-shared key for the WDS WLAN service wds-test as **testsecret**:

```
EWC.enterasys.com# wlans
EWC.enterasys.com:wlans# wds-test
EWC.enterasys.com:wlans:wds-test# psk testsecret
EWC.enterasys.com:wlans:wds-test# apply
EWC.enterasys.com:wlans:wds-test# show
Service type: wds
Pre-shared Key: testsecret
Name: wds-test
Enable status: enable
Pre-shared Key: testsecret
SSID: wdstest
EWC.enterasys.com:wlans:wds-test#
```

Note: After you run the **psk** command, you must run the **apply** command to implement the changes.

19.6.13 qos-policy

The **qos-policy** command moves you to the **wlan:<WLAN-service-name>:qos_policy** context, which provides commands for the configuration of QoS support options for the WLAN service.

The following commands are available in the **wlan:<WLAN-service-name>:qos_policy** context.

- dot11e
- downlink
- flex-client-access
- legacy
- priority-map
- priority-override
- priority-override-dscp
- priority-override-up
- turbo-voice
- uapsd
- uplink
- wmm
- video-admission-control
- voice-admission-control

19.6.13.1 dot11e

Use the **dot11e** command to enable or disable 802.11e radio QoS support. The **dot11e** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
dot11e enable | disable
```

Parameters

enable | disable	Specify to enable or disable 802.11e radio QoS support

Examples

The following example enables 802.11e support on the Enterasys Wireless Controller:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# dot11e enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show dot11e
802.11e: enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy#
```

Note: After you run the **dot11e** command, you must run the **apply** command to implement the changes.

19.6.13.2 downlink

Use the **downlink** command to manage downlink policer action for this WLANS. The **downlink** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
downlink downgrade | drop | do-nothing
```

Parameters

downgrade	Specifies that the transmission's data packets are forced to be downgraded to the next priority when a TSPEC violation is discovered
drop	Specifies that the transmission's data packets are forced to be dropped when a TSPEC violation is discovered
do-nothing	Specifies that the TSPEC violations are allowed to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions

Examples

The following example defines the QoS downlink policy to drop the transmission's data packets when a TSPEC violation is discovered:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# downlink drop
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
```

Note: After you run the **downlink** command, you must run the **apply** command to implement the changes.

19.6.13.3 flex-client-access

Use the **flex-client-access** command to enable or disable flexible client access to the wireless medium. The **flex-client-access** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
flex-client-access enable | disable
```

Parameters

enable | disable	Enables or disables flexible client access to the wireless medium

Examples

The following example enables flexible client access to the wireless medium:

```
EWC.enterasys.com:wlans:test:qos-policy# flex-client-access enable
EWC.enterasys.com:wlans:test:qos-policy# apply
EWC.enterasys.com:wlans:test:qos-policy# show flex-client-access
Flex client access: enable
```

Note: After you run the **flex-client-access** command, you must run the **apply** command to implement the changes.

19.6.13.4 legacy

Use the **legacy** command to enable or disable the legacy solution, which gives all packets on the VNS high priority. The **legacy** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
legacy enable | disable
```

Parameters

enable | disable	Enables or disables flexible client access to the wireless medium

Examples

The following example enables the legacy solution for the VNS

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# legacy enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show legacy
Legacy: enable
```

Note: After you run the **legacy** command, you must run the **apply** command to implement the changes.

19.6.13.5 priority-map

Use the **priority-map** command to configure Differentiated Service Code Point (DSCP) classification by mapping Service Class user priority levels to DSCP codepoints. The **priority-map** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
priority-map dscp <0-64> user-priority <0-7>
```

Parameters

dscp <0-64>	Specifies a DSCP codepoint value
user-priority <0-7>	Specifies the Service Class value to be assigned to a DSCP codepoint

Examples

The following example assigns a Service class of 7 to DSCP codepoint 24:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# priority-map dscp 24 user-priority 7
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show priority-map
DSCP CLASSIFICATION
        dscp-marking    service-class
        0                02
        1                00
.
        23               00
        24               07
        25               00
```

Note: After you run the **priority-map** command, you must run the **apply** command to implement the changes.

19.6.13.6 priority-override

Use the **priority-override** command to override the priority for all packets in the WLANS. The **priority-override** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
priority-override enable | disable
```

Parameters

enable | disable	Enables or disables priority override for all packets in the WLANS

Examples

The following example overrides priority for all packets on WLANS CNL-7-CP:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# priority-override enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show priority-override
Priority override: enable
```

Note: After you run the **priority-override** command, you must run the **apply** command to implement the changes.

19.6.13.7 priority-override-dscp

Use the **priority-override-dscp** command to override existing DSCP codepoint assignments for priority processing and use a single DSCP codepoint for the WLANS. The **priority-override-dscp** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
priority-override-dscp <0-64>
```

Parameters

<0-64>	Specifies a DSCP codepoint value. Default value: 0.

Usage

This command is only active if the **priority-override** command has been enabled. For more information, see "priority-override" on page 19-48.

Examples

The following example overrides all existing DSCP codepoint assignments and uses DSCP codepoint 2 for the CNL-7-CP WLANS:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# priority-override-dscp 2
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show priority-override-dscp
DSCP marking: 2
```

Note: After you run the **priority-override-dscp** command, you must run the **apply** command to implement the changes.

19.6.13.8 priority-override-up

Use the **priority-override-up** command to override existing Service Class settings for priority processing and configure a single Service Class value for the WLANS. The **priority-override-up** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
priority-override-up <0-7>
```

Parameters

<0-7>	Specifies a Service Class value. Default value: 1.

Usage

This command is only active if the **priority-override** command has been enabled. For more information, see "priority-override" on page 19-48.

Examples

The following example overrides all existing Service Class settings and configures a single Service Class of 4 for the CNL-7-CP WLANS:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos_policy# priority-override-up 4
EWC.enterasys.com:wlans:CNL-7-CP:qos_policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos_policy# show priority-override-up
Service class: 4
```

Note: After you run the **priority-override-up** command, you must run the **apply** command to implement the changes.

19.6.13.9 turbo-voice

Use the **turbo-voice** command to enable or disable Turbo Voice optimization. The **turbo-voice** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
turbo-voice enable | disable
```

Parameters

enable | disable	Enables or disables Turbo Voice optimization on the WLANS

Usage

This command is only active when either the **wmm**, **802.11e**, or **legacy** commands have been enabled.

Examples

The following example enables Turbo Voice on the CNL-7-CP WLANS:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# turbo-voice enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show turbo-voice
Turbo voice: enable
```

Note: After you run the **turbo-voice** command, you must run the **apply** command to implement the changes.

19.6.13.10 uapsd

Use the **uapsd** command to enable Unscheduled Automatic Power Save Delivery (U-APSD) on the VNS. Use the **no** form of the command to disable it. The **uapsd** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
uapsd enable | disable
```

Parameters

enable | disable	Enables or disables U-APSD. Default value: disabled.

Usage

This command is only available when either the **802.11e** or **wmm** commands have been enabled. For more information see "dot11e" on page 19-46 and "wmm" on page 19-52.

Examples

The following example enables U-APSD on the CNL-7-CP WLANS:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# uapsd enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show uspsd
Enable U-APSD: enable
```

Note: After you run the **uapsd** command, you must run the **apply** command to implement the changes.

19.6.13.11 uplink

Use the **uplink** command to manage the uplink policer action for this WLANS. The **uplink** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
uplink delts | do-nothing
```

Parameters

delts	Specifies that TSPEC violations will end when they are discovered. This action deletes the TSPEC.
do-nothing	Specifies that TSPEC violations are allowed to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.

Usage

This command is only active if the Video and Voice Admission Control is set to enable. See "video-admission-control" on page 19-52 and "voice-admission-control" on page 19-53

Examples

The following example defines the uplink policer action to end TSPEC violations by deleting the TSPEC for the CNL-7-CP WLANS:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# uplink delts
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
```

Note: After you run the **uplink** command, you must run the **apply** command to implement the changes.

19.6.13.12 wmm

Use the **wmm** command to enable Wi-Fi Multimedia enhancements for audio, video, and voice applications. The **wmm** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
wmm enable | disable
```

Parameters

enable | disable	Enables or disables Wi-Fi Multimedia enhancements on the WLANS

Examples

The following example enables Wi-Fi Multimedia enhancements on the CNL-7-CP WLANS:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# wmm enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show wmm
WMM: enable
```

Note: After you run the **wmm** command, you must run the **apply** command to implement the changes.

19.6.13.13 video-admission-control

Use the **video-admission-control** command to enable or disable global admission control for video. The **video-admission-control** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
video-admission-control enable | disable
```

Parameters

enable | disable	Enables or disables video admission control for the WLANS

Usage

Enabling video admission control automatically enables voice admission control. Disabling video admission control automatically disables voice admission control.

Examples

The following example enables global admission control for video:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# video-admission-control enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show video-admission-control
Use Global Admission Control for Video (VI): enable
```

Note: After you run the **video-admission-control** command, you must run the **apply** command to implement the changes.

19.6.13.14 voice-admission-control

Use the **voice-admission-control** command to enable global admission control for voice for WLANS. The **voice-admission-control** command is accessible from the **wlan:<WLAN-service-name>:qos-policy** context of the CLI.

Syntax

```
voice-admission-control enable | disable
```

Parameters

enable | disable	Enables or disables global admission control for voice for WLANS.

Usage

This command is only available when either the **802.11e** or **wmm** commands have been enabled. For more information, see "dot11e" on page 19-46 and "wmm" on page 19-52.

Examples

The following example enables global admission control for voice for the CNL-7-CP WLANS:

```
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# voice-admission-control enable
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# apply
EWC.enterasys.com:wlans:CNL-7-CP:qos-policy# show voice-admission-control
Use Global Admission Control for Voice (VO): enable
```

Note: After you run the **voice-admission-control** command, you must run the **apply** command to implement the changes.

19.6.14 remoteable

Use the **remoteable** command to enable or disable the SSID advertisement to the mobility domain. The **remoteable** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI.

Syntax

```
remoteable enable | disable
```

Parameters

enable | disable	Enables or disables the SSID advertisement to the mobility domain.

Examples

The following example enables the SSID advertisement for the CNL-7-CP WLANS:

```
EWC.enterasys.com:wlans:CNL-7-CP# remoteable enable
EWC.enterasys.com:wlans:CNL-7-CP# apply
EWC.enterasys.com:wlans:CNL-7-CP# show remoteable
Remote Service: enable
```

Note: After you run the **remoteable** command, you must run the **apply** command to implement the changes.

19.6.15 rf

The **rf** command moves you to the **wlan:<WLAN-service-name>:rf** context, which contains commands to configure RF options for the WLAN service.

The following commands are available in the **wlan:<WLAN-service-name>:rf** context.

- 11h-power-reduction
- 11h-support
- energy-save-mode
- process-client-ie
- show
- ssid-suppress

19.6.15.1 11h-power-reduction

Use the **11h-power-reduction** command to enable or disable automatic power reduction of transmissions using the 802.11h standard. The **11h-power-reduction** command is accessible from the **wlan:<WLAN-service-name>:rf** context of the CLI.

Syntax

```
11h-power-reduction enable | disable
```

Parameters

enable | disable	Enables or disables automatic power reduction of transmissions using the 802.11h standard

Examples

The following example enables the power reduction feature on the WLAN service:

```
EWC.enterasys.com:wlans:test:rf# 11h-power-reduction enable
EWC.enterasys.com:wlans:test:rf# apply
EWC.enterasys.com:wlans:test:rf# show 11h-power-reduction
Apply power reduction to 11h clients: enable
```

Note: After you run the **11h-power-reduction** command, you must run the **apply** command to implement the changes.

19.6.15.2 11h-support

802.11h support on the Enterasys Wireless Controller will allow clients to operate with the maximum available transmission power in 5Ghz bands. The **11h-support** command is accessible from the **wlan:<WLAN-service-name>:rf** context of the CLI.

Use the **11h-support** command to enable 802.11h support on the WLAN service.

Syntax

```
11h-support enable | disable
```

Parameters

enable | disable	Enables or disables 802.11h support on the Enterasys Wireless Controller

Examples

The following example enables 802.11h support on the WLAN service:

```
EWC.enterasys.com:wlans:test:rf# 11h-support enable
EWC.enterasys.com:wlans:test:rf# apply
EWC.enterasys.com:wlans:test:rf# show 11h-support
Enable 11h support: enable
```

Note: After you run the **11h-support** command, you must run the **apply** command to implement the changes.

19.6.15.3 energy-save-mode

Use the **energy-save-mode** command to enable or disable the AP energy saving mode. The **energy-save-mode** command is accessible from the **wlan:<WLAN-service-name>:rf** context of the CLI.

Syntax

```
energy-save-mode enable | disable
```

Parameters

enable | disable	Enables or disables the AP energy saving mode on the WLAN service.

Examples

The following example enables AP energy saving mode:

```
EWC.enterasys.com:wlans:CNL-7-CP:rf# energy-save-mode enable
```

19.6.15.4 process-client-ie

Use the **process-client-ie** command to enable or disable the processing of Information Element 10 (IE 10). The **process-client-ie** command is accessible from the **wlan:<WLAN-service-name>:rf** context of the CLI.

Syntax

```
process-client-ie enable | disable
```

Parameters

enable | disable	Enables or disables the processing of Information Element 10 (IE 10) on the Enterasys Wireless Controller

Examples

The following example enables IE 10 processing:

```
EWC.enterasys.com:wlans:CNL-7-CP:rf# process-client-ie enable
EWC.enterasys.com:wlans:CNL-7-CP:rf# apply
```

Note: After you run the **process-client-ie** command, you must run the **apply** command to implement the changes.

19.6.15.5 show

Use the **show** command to display the current RF settings of the specified individual WLAN service. The **show** command is accessible from the **wlan:<WLAN-service-name>:rf** context of the CLI.

Examples

The following example displays the current RF settings for the WLAN service named “test.”

```
EWC.enterasys.com:wlans:test:rf# show
```

```
Process client IE requests: disable
Enable 11h support: disable
Apply power reduction to 11h clients: disable
Suppress SSID: disable
Energy save mode: disable
```

19.6.15.6 ssid-suppress

Use the **ssid-suppress** command to allow or prevent the SSID from being broadcast by the Wireless AP. The **ssid-suppress** command is accessible from the **wlan:<WLAN-service-name>:rf** context of the CLI.

Syntax

```
ssid-suppress enable | disable
```

Parameters

enable | disable	Enables or disables the suppression of broadcast of the SSID

Examples

The following example prevents SSID broadcasts

```
EWC.enterasys.com:wlans:CNL6-AAA# ssid-suppress enable
EWC.enterasys.com:wlans:CNL6-AAA# apply
```

Note: After you run the **ssid-suppress** command, you must run the **apply** command to implement the changes.

19.6.16 show

Use the **wlan:<WLAN-service-name>:show** command to display the current settings of the specified individual WLAN service. The **show** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI.

Examples

The following example displays the current WLAN service settings for the WLAN service named "test."

```
EWC.enterasys.com:wlans:test# show
Service type: std
Name: test
Synchronize: disable
Enable status: enable
Wireless AP Services:
Wireless AP: 04099202012xxxxx
Wireless AP: 04099202012xxxxx
Wireless AP: 05000092030xxxxx
SSID: _ssidtest
pre-authentication timeout(minutes): 5
```

```
post-authentication timeout(minutes): 30
session timeout(minutes): 0
Block MU to MU traffic: disable
```

This example displays the settings for the dynamic mesh WLAN service named mesh1-wlan.

```
EWC.enterasys.com:wlans:mesh1-wlan# show
Service type: mesh
Pre-shared Key:
SSID: mesh1
Backhaul Radio Band: a
Name: mesh1-wlan
Enable/disable WLAN Service: enable
aplist-wds 0500008043050236  portal wkgbridge on
Radio Mode: off
```

19.6.17 ssid

Use the **ssid** command to specify the Service Set Identifier (SSID) for the WLAN service being configured. The **ssid** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI.

Syntax

```
ssid <string>
```

Parameters

<string>	Specifies a string for the SSID. The SSID string can range in length from 1 to 32 characters.

Examples

The following example specifies the SSID and then displays it

```
EWC.enterasys.com:wlans:test# ssid testssid
EWC.enterasys.com:wlans:test# apply
EWC.enterasys.com:wlans:test# show ssid
SSID: testssid
```

Note: After you run the **ssid** command, you must run the **apply** command to implement the changes.

19.6.18 status

Use the **status** command to enable or disable this WLAN service. The status command is accessible from the **wlans:<WLAN-service-name>** context of the CLI.

Syntax

```
status enable | disable
```

Parameters

enable | disable	Enables or disables this WLAN service

Examples

The following example enables this WLAN service

```
EWC.enterasys.com:wlans:test# status enable
EWC.enterasys.com:wlans:test# apply
EWC.enterasys.com:wlans:test# show status
Enable status: enable
```

Note: After you run the **status** command, you must run the **apply** command to implement the changes.

19.6.19 sync

Use the **sync** command to enable or disable automatic synchronization of this WLAN service across paired Enterasys Wireless Controllers. The **sync** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI.

Syntax

```
sync enable | disable
```

Parameters

enable | disable	Enables or disables automatic synchronization of this WLAN service across paired Enterasys Wireless Controllers

Examples

The following example enables synchronization for this WLAN service

```
EWC.enterasys.com:wlans:test# sync enable
EWC.enterasys.com:wlans:test# apply
EWC.enterasys.com:wlans:test# show sync
Synchronize: enable
```

Note: After you run the **sync** command, you must run the **apply** command to implement the changes.

19.6.20 timeout-post

Use the **timeout-post** command to set the post-authentication timeout value (in minutes) for this WLAN service. The **timeout-post** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI.

Syntax

```
timeout-post <0-999999>
```

Parameters

<0-999999>	Specify the post-authentication timeout value in minutes for this WLAN service

Examples

The following example sets the post-authentication timeout value to 10 minutes for this WLAN service:

```
EWC.enterasys.com:wlans:test# timeout-post 10
EWC.enterasys.com:wlans:test# apply
```

Note: After you run the **timeout-post** command, you must run the **apply** command to implement the changes.

19.6.21 timeout-pre

Use the **timeout-pre** command to set the pre-authentication timeout value (in minutes) for this WLAN service. The **timeout-pre** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI.

Syntax

```
timeout-pre <0-999999>
```

Parameters

<0-999999>	Specify the pre-authentication timeout value in minutes for this WLAN service

Examples

The following example sets the pre-authentication timeout value to 10 minutes for this WLAN service:

```
EWC.enterasys.com:wlans:test# timeout-pre 10
EWC.enterasys.com:wlans:test# apply
EWC.enterasys.com:wlans:test# show timeout-pre
pre-authentication timeout(minutes): 10
```

Note: After you run the **timeout-pre** command, you must run the **apply** command to implement the changes.

19.6.22 timeout-session

Use the **timeout-session** command to set the session timeout value (in minutes) for this WLAN service. The **timeout-session** command is accessible from the **wlan:<WLAN-service-name>** context of the CLI.

Syntax

```
timeout-session <0-999999>
```

Parameters

<0-999999>	Specify the session timeout value in minutes for this WLAN service

Examples

The following example sets the session timeout value to never for this WLAN service:

```
EWC.enterasys.com:wlans:test# timeout-session 0
EWC.enterasys.com:wlans:test# apply
EWC.enterasys.com:wlans:test# show timeout-session
session timeout(minutes): 0
```

Note: After you run the **timeout-session** command, you must run the **apply** command to implement the changes.

20

policy Commands

This section describes commands used to define and configure policy for the Enterasys Wireless Controller. These commands are located in the **policy** context of the CLI. Execute the **policy** command at the root level to enter policy context. Refer to Section 6.10, "Configuring Policy," in the Enterasys Wireless Controller User Guide for more information about policy configuration.

A policy is a collection of attributes and rules that determine how the traffic, of users accessing the wired network through the WLAN service, is handled. Policy assignment ensures that the correct topology and traffic behavior are applied to a user regardless of SSID or VNS assignment. Traffic behavior is defined in policy by configuring a rate control setting and filter rules for the AC or AP.

Policies do not need to be fully specified. Unspecified attributes are retained by the user or inherited from the global default-policy. Refer to "default-policy" on page 18-6 for information on configuring the global default-policy.

A policy either specifies or defaults to:

- A topology
- An inbound and outbound rate control profile
- A set of filters

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

Note: The **policy** context was introduced with V7.0.

The following commands are available in the **policy** context:

- create
- delete
- enable-advance-filtering
- show
- <named-policy> — See <named-policy> for commands in the **topology:<named-policy>** context.

20.1 create

Use the **create** command to create a new policy, specifying a name for the new policy. The **create** command is accessible from the policy context.

Syntax

```
create <policy-name>
```

Parameters

<policy-name>	Specifies the name of the policy. A policy name can be made up of all alpha-numeric characters, as well as special characters: -!#$:

Usage

The default values for a newly created policy are:

- Default Filter: disabled
- AC Filter: Controller filtering is active, with a default filter of deny in both directions
- Ingress rate profile: no-change
- Egress rate profile: no-change
- Topology: no-change
- Filtering on the AP: disabled
- Synchronization: disabled

Examples

The following example creates and then displays the details of a policy named **p6**:

```
EWC.enterasys.com:policy# create p6
EWC.enterasys.com:policy# show p6
Assigned topology: no change
Ingress rate profile: no change
Egress rate profile: no change
Filter settings: enable
Enable AP filtering: disable
Name: p6
EWC.enterasys.com:policy# show p6 acfilter
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 2 (default) proto none 0.0.0.0  all_ports in none out src allow
```

20.2 delete

Use the **delete** command to delete a policy, specifying the name of the policy to be deleted. The **delete** command is accessible from the policy context of the CLI.

Syntax

```
delete <policy-name>
```

Parameters

<policy-name>	Specifies the name of the policy to delete

The following example deletes the policy named **p6**.

```
EWC.enterasys.com:policy# delete p6
```

20.3 enable-advance-filtering

Use this command to enable advanced filtering definitions. The **enable-advance-filtering** command is accessible from the policy context of the CLI.

Syntax

```
enable-advance-filtering
```

Parameters

None.

Usage

By default, when v7.41 is installed, the controller will be in compatibility mode. After all controllers and APs in a deployment have been upgraded to v7.41, advanced filtering definitions can be enabled with this command. After advanced filtering has been enabled, the controller can be returned to compatibility mode only by importing a backup configuration.

Examples

This example enables advanced filtering definitions.

```
EWC.enterasys.com:policy# enable-advance-filtering
```

20.4 show

Use the show command to display policy configuration information. The **show** command is accessible from within the the policy context.

Syntax

```
show {policy | <policy-name>}
```

Parameters

policy	Specifies that information for all configured policies should be displayed
<policy-name>	Specifies that information for the named policy should be displayed.

Examples

The following example displays the current list of policy configuration information.

```
EWC:policy# show
Advanced filtering: disabled

Policy name  Topology     Ingress rate profile  Egress rate profile  Mode    Filter defined

Unauth       Seg1_Routed  Ingress              Egress               routed  Yes
Auth         Seg1_Routed  Ingress              Egress               routed  Yes
Quarantine   Seg1_Routed  Ingress              Egress               routed  Yes
```

The following example displays configuration information for the policy named **Quarantine**:

```
EWC:policy# show Quarantine
Assigned topology: Seg1_Routed
Ingress rate profile: Ingress
Egress rate profile: Egress
Filter settings: enable
Enable AP filtering: disable
Name: Quarantine
```

20.5 <named-policy>

The **<named-policy>** command, where <named-policy> refers to the name of a given policy, provides access to the policy:<named-policy> context.

The policy:<named-policy> context provides commands for the configuration of the <named-policy>. A <named-policy> must first be created using the **create** command in the policy context. Once created it becomes available as a command, allowing access to the policy:<named-policy> context for that policy. For example, to enter the <named-policy> context for the policy named **p6**, use the command **p6** from the policy context, created using the **create p6** command.

Note: After you have completed configuration changes for a <named-policy>, you must run the **apply** command before exiting the policy:<named-policy> context to implement the changes.

The following commands are available in the **policy:<named-policy>** context.

- show
- filter-status
- name
- sync
- acfilters — See acfilters for commands in the **policy:<named-policy>:acfilters** context.
- rateprf-in
- rateprf-out
- topology-name
- ulfilterap

- apcustom
- apfilters — See apfilters for commands in the **policy:<named-policy>:apfilters** context.

20.5.1 show

Use the **show** command to display the <named-policy> configuration information for the current **policy:<named-policy>** context. The **show** command is accessible from within the the **policy:<named-policy>** context.

Syntax

```
show
```

Parameters

None.

Examples

The following example displays the **p1** policy configuration from within the **p1** policy:<named-policy> context:

```
EWC.enterasys.com:policy# p1
EWC.enterasys.com:policy:p1# show
Assigned topology: no change
Ingress rate profile: snmpDefault.0
Egress rate profile: snmpDefault.64
Do not change filter settings when this Policy is applied: disable
Enable AP filtering: disable
Name: p1
Synchronize: disable
EWC.enterasys.com:policy:p1#
```

20.5.2 filter-status

Use the **filter-status** command to configure the filter feature setting. The **filter-status** command is accessible from within the the **policy:<named-policy>** context.

Syntax

```
filter-status {enable | no-change}
```

Parameters

enable	Enable AC and AP filter rule modification for the policy being configured.
no-change	Keep the previous filter in use.

Usage

If the **filter-status** command is set to enabled, the **acfilters** and **ulfilterap** commands are available so that you canmodify the current AC and AP filter configuration.

If the **filter-status** command is set to no-change, any filters that exist in the previous policy are applied to this user. For example, if the previous policy is the default-policy, default-policy filters are applied to this user.

The **show <named-policy>** command, within the policy context, and the **show** command, within a policy:<named-policy> context, specify the current filter-status command setting with the line "Do not change filter settings when this Policy is applied:".

Examples

The following example enables access to AC and AP filter configuration within the p1 <named-policy> context:

```
EWC.enterasys.com:policy:p1# filter-status enable
EWC.enterasys.com:policy:p1# apply
EWC.enterasys.com:policy:p1# show
Assigned topology: Seg1_Routed
Ingress rate profile: no change
Egress rate profile: no change
Do not change filter settings when this Policy is applied: enable
Name: Auth
Synchronize: disable
```

20.5.3 name

Use the **name** command to change the name of a policy. The **name** command is accessible from within the the **policy:<named-policy>** context.

Syntax

```
name <new-name>
```

Parameters

<new-name>	Specifies the new name for this <named-policy>.

Usage

You must enter the **apply** command before exiting the **policy:<named-policy>** context for the policy name change to take affect. The CLI prompt will not change until you exit and re-enter the **policy:<named-policy>** context.

Examples

The following example:

- Renames the policy **p1** to **policy1**
- Applies the change
- Displays the **policy1** configuration
- Exits policy:<named-policy> context
- Re-enters the policy:<named-policy> context as **policy1**

```
EWC.enterasys.com:policy# p1
```

```
EWC.enterasys.com:policy:p1# name policy1
EWC.enterasys.com:policy:p1# apply
EWC.enterasys.com:policy:p1# show
Assigned topology: no change
Ingress rate profile: no change
Egress rate profile: no change
Do not change filter settings when this Policy is applied: disable
Enable AP filtering: disable
Name: policy1
Synchronize: disable
EWC.enterasys.com:policy:p1# exit
EWC.enterasys.com:policy# policy1
EWC.enterasys.com:policy:policy1#
```

20.5.4 sync

Use the sync command to enable or disable automatic synchronization of this <named-policy> across paired controllers. Refer to Section 6.2.7, "Using the Sync Summary," in the Enterasys Wireless Controller User Guide for more information about synchronization of policies.

The **sync** command is accessible from within the **policy:<named-policy>** context.

Syntax

```
sync {enable | disable}
```

Parameters

enable | disable	Enables or disables automatic synchronization of this <named-policy> across paired controllers.

Examples

The following example enables the synchronization of the **p1** policy across controllers:

```
EWC.enterasys.com:policy:p1# sync enable
EWC.enterasys.com:policy:p1# apply
EWC.enterasys.com:policy:p1# show
Assigned topology: no change
Ingress rate profile: no change
Egress rate profile: no change
Do not change filter settings when this Policy is applied: disable
Enable AP filtering: disable
Name: p1
Synchronize: enable
EWC.enterasys.com:policy:p1#
```

20.5.5 acfilters

Use the **acfilters** command to enter the **policy:<named-policy>:acfilters** context for the configuring of AC filters. AC filter rules are applied at the controller. The **acfilters** command is accessible from within the the **policy:<named-policy>** context.

Notes: AC filtering is not available when the associated topology is configured for Bridge at AP. AC filtering is available when the associated topology is set to either Bridge at AC or Routed.

The **acfilter** command has been replaced by **acfilters**. **acfilter** is deprecated.

The following commands are available in the **policy:<named-policy>:acfilters** context.

- create
- config
- delete
- move

Syntax

```
acfilters
```

Parameters

None.

Usage

The "no-change" filter setting must be disabled using the **filter disable** command for the **acfilters** command to be visible in the CLI.

Examples

The following example enters the policy:<named-policy>:acfilters context for the **p1** <named-policy>:

```
EWC.enterasys.com:policy:p1# acfilters
EWC.enterasys.com:policy:p1:acfilters#
```

20.5.5.1 create

Use the **create** command to create, insert, or append a new filter rule into an AC filter list for a <named-policy>. The **create** command is accessible from within the **policy:<named-policy>:acfilters** context.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode syntax:

```
create <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|dst) out (none|src)
(allow | deny)
```

Advanced mode syntax:

```
create <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|src|dst|both) out
(none|src|dst|both) (allow | deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <protocol>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **all** - All protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
<ipaddress/mask>	Specifies an IP address and mask for this filter rule.
interface-subnet	Specifies that the IP address and mask configured for the associated topology will be used for this filter rule.
interface-ip	Specifies the IP address of the associated topology will be used for this filter rule.
port <port> [<port>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type <type> [<type>]	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0 - 255.
Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow. — **in** specifies a packet flow from the AP to the AC. **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.

Basic: out (none|src) Advanced: out (none|src|dst|both)	Specifies the direction of packet flow. — **out** specifies a packet flow from the AC to the AP. **none** specifies that the **out** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
allow | deny	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified rule position already contains a filter rule, specifying a rule using this command inserts a rule in the specified position in the list and resequences all rules below this filter down by one position. Use the **create** command to insert or append a rule at the specified position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example shows the default filter rules applied to a policy.

```
EWC.enterasys.com:policy# create p6
EWC.enterasys.com:policy# show p6 acfilter
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 2 (default) proto none 0.0.0.0  all_ports in none out src allow
```

The following example creates a (basic mode) filter rule 1 that allows UDP traffic in both directions from IP address 192.168.10.0/24 for ports 10 through 2000:

```
EWC.enterasys.com:policy:Auth:acfilters# create 1 proto udp 192.168.10.0/24 port
10 2000 in dst out src allow
EWC.enterasys.com:policy:Auth:acfilters# apply
EWC.enterasys.com:policy:Auth:acfilters# show
Enable AP filtering: disable
filter 1 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src allow
filter 2 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 3 (default) proto none 0.0.0.0  all_ports in none out src allow
```

The following example creates a filter rule 1 that is inserted into the rule list at position 1 resequencing the current rule 1. This filter rule allows TCP traffic in both directions from IP address 192.168.0.0/16 for ports 10 through 20000:

```
EWC.enterasys.com:policy:Auth:acfilters# create 1 proto tcp 192.168.0.0/16 port
10 2000 in dst out src allow
EWC.enterasys.com:policy:Auth:acfilters# show
Enable AP filtering: disable
```

```
filter 1 proto tcp 192.168.0.0 255.255.0.0 port 10 2000 in dst out src allow
filter 2 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src allow
filter 3 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0  all_ports in none out src allow
```

20.5.5.2 config

Use the **config** command to modify an existing AC filter rule for this <named-policy>. The **config** command is accessible from within the **policy:<named-policy>:acfilters** context.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode syntax:

```
config <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|dst) out (none|src)
(allow|deny)
```

Advanced mode syntax:

```
config <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|src|dst|both) out
(none|src|dst|both) (allow|deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <protocol>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **all** - All protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
<ipaddress/mask>	Specifies an IP address and mask for this filter.
interface-subnet	Specifies that the IP address and mask configured for the associated topology will be used for this filter rule.
interface-ip	Specifies the IP address of the associated topology will be used for this filter rule.
port <port> [<port>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a port range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.

type <type> [<type>]	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0 - 255.
Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow. — **in** specifies a packet flow from the AP to the AC. **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
Basic: out (none|src) Advanced: out (none|src|dst|both)	Specifies the direction of packet flow. — **out** specifies a packet flow from the AC to the AP. **none** specifies that the **out** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
allow | deny	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified rule position already contains a filter rule, the **config** command overwrites the existing rule. Use the **create** command to insert or append a rule at the specified position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example overwrites a pre-existing filter rule 1 with a rule that allows ICMP traffic types 9 through 31 in both directions for the associated topology's interface subnet and mask:

```
EWC.enterasys.com:policy:p1:acfilters# config 1 proto icmp interface-subnet type
9 31 in dst out src allow
EWC.enterasys.com:policy:p1:acfilters# apply
EWC.enterasys.com:policy:p1:acfilters# show
Enable AP filtering: disable
filter 1 proto icmp interface-subnet type 9 31 in dst out src allow
filter 2 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src allow
filter 3 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0  all_ports in none out src allow
```

20.5.5.3 delete

Use the **delete** command to remove a filter rule from the filter list. The **delete** command is accessible from within the **policy:<named-policy>:acfilters** context.

Syntax

```
delete <pos>
```

Parameters

<pos>	Specifies the filter rule list position of the filter to be deleted. Valid values are from 0 -255.

Examples

The following example deletes filter rule 1 and displays the remaining default deny all rule:

```
EWC.enterasys.com:policy:p1:acfilters# delete 1
EWC.enterasys.com:policy:p1:acfilters# show
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0  all_ports both deny
```

20.5.5.4 move

Use the **move** command to move a filter rule from its current position in the filter list to the specified filter list position. The **move** command is accessible from within the **policy:<named-policy>:acfilters** context.

Syntax

```
move <cur-pos> <new-pos>
```

Parameters

<cur-pos> <new-pos>	Specifies the current position in the filter list of the rule to be moved, followed by the new list position for the filter rule. Valid values are from 0 -255.

Examples

The following example:

- Moves the rule in list position 2 to list position 1
- Displays the new list ordering:

```
EWC.enterasys.com:policy:p1:acfilters# move 2 1
EWC.enterasys.com:policy:p1:acfilters# show
Enable AP filtering: disable
filter 1 proto udp 192.168.10.0 255.255.255.0 port 10 2000 both allow
filter 2 proto tcp 192.168.10.0 255.255.255.0 port 10 2000 both allow
filter 3 (default) proto none 0.0.0.0  all_ports both deny
EWC.enterasys.com:policy:p1:acfilters#
```

20.5.6 rateprf-in

Use the **rateprf-in** command to associate an already existing rate profile with a policy as an ingress rate profile. The **rateprf-in** command is accessible from the **policy:<named-policy>** context.

Syntax

```
rateprf-in <profile> | no-change
```

Parameters

<profile>	Specifies the ingress rate profile to associate with this policy:<named-policy> context.
no-change	Specifies that no rate profile change is associated with this policy. When applying this policy to a user at runtime, the user retains the inbound rate profile currently enforced.

Usage

Refer to "rateprofile" on page 18-32 for rate profile configuration information.

Examples

The following example configures the **p1** <named-policy> with the **Unlimited** ingress rate profile:

```
EWC.enterasys.com:policy:p1# rateprf-in Unlimited
EWC.enterasys.com:policy:p1# apply
EWC.enterasys.com:policy:p1# show
Assigned topology: no change
Ingress rate profile: Unlimited
Egress rate profile: no change
Do not change filter settings when this Policy is applied: disable
Enable AP filtering: disable
Name: p1
Synchronize: disable
EWC.enterasys.com:policy:p1#
```

20.5.7 rateprf-out

Use the **rateprf-out** command to associate an already existing rate profile with a policy as an egress rate profile. The **rateprf-out** command is accessible from the **policy:<named-policy>** context.

Syntax

```
rateprf-out <profile> | no-change
```

Parameters

<profile>	Specifies the egress rate profile to associate with this policy:<named-policy> context.

no-change	Specifies that no rate profile change is associated with this policy. When applying this policy to a user at runtime, the user retains the egress rate profile currently enforced.

Usage

Refer to "rateprofile" on page 18-32 for Rate Profile Configuration Information.

Examples

The following example configures the **p1** <named-policy> with the **Unlimited** egress rate profile:

```
EWC.enterasys.com:policy:p1# rateprf-out Unlimited
EWC.enterasys.com:policy:p1# apply
EWC.enterasys.com:policy:p1# show
Assigned topology: no change
Ingress rate profile: Unlimited
Egress rate profile: Unlimited
Do not change filter settings when this Policy is applied: disable
Enable AP filtering: disable
Name: p1
Synchronize: disable
EWC.enterasys.com:policy:p1#
```

20.5.8 topology-name

Use the **topology-name** command to associate an already existing topology with a policy. The **topology-name** command is accessible from the **policy:<named-policy>** context.

Syntax

```
topology-name <topology> | no-change
```

Parameters

<topology>	Specifies the name of the topology to configure for this policy:<named-policy> context.
no-change	Specifies that no topology change is associated with this policy. When applying this policy to a user at runtime, the user retains the topology currently enforced.

Usage

Refer to Chapter 21, **topology Commands** for information on configuring topologies.

Examples

The following example configures the **p1** <named-policy> with the **guestPortal** topology:

```
EWC.enterasys.com:policy:p1# topology-name guestPortal
EWC.enterasys.com:policy:p1# apply
EWC.enterasys.com:policy:p1# show
```

```
Assigned topology: guestPortal
Ingress rate profile: no change
Egress rate profile: no change
Do not change filter settings when this Policy is applied: disable
Enable AP filtering: disable
Name: p1
Synchronize: disable
EWC.enterasys.com:policy:p1#
```

20.5.9 ulfilterap

Use the **ulfilterap** command to enable filtering on the AP. The **ulfilterap** command is accessible from the **policy:<named-policy>** context.

Syntax

```
ulfilterap {enable | disable}
```

Parameters

enable | disable	Provides for the enabling or disabling of filtering on the AP for this policy:<named-policy> context.

Usage

When filtering is enabled on the AP, wireless APs obtain client filter information from the Enterasys Wireless Controller. Filter rules defined on the controller are applied by wireless APs. In addition, direct inter-Wireless AP communication allows Wireless APs to exchange client filter information as clients roam from one Wireless AP to another.

The filter setting feature must be disabled using the **filter disable** command for the **apfilters** command to be visible in the CLI.

See "apcustom" on page 20-16 to apply custom filters for the AP.

Examples

The following example enables filtering on the AP for this policy:p1 context:

```
EWC.enterasys.com:policy:p1# ulfilterap enable
EWC.enterasys.com:policy:p1#
```

20.5.10 apcustom

Use the **apcustom** command to enable AP custom filters. The **apcustom** command is accessible from the **policy:<named-policy>** context.

Syntax

```
apcustom {enable | disable}
```

Parameters

enable | disable	Provides for the enabling or disabling of AP custom filters for this policy:<named-policy> context.

Usage

Enabling AP custom filters provides for the ability to access the **policy:<named-policy>:apfilters** context using the **apfilters** command. The **apfilters** command allows for the configuration of additional filters for the APs.

Filtering on the AP must be enabled using the **ulfilterap enable** command for the **apcustom** command to be visible in the CLI.

Examples

The following example enables AP custom filters for the policy:p1:apfilters context:

```
EWC.enterasys.com:policy:p1# ulfilterap enable
EWC.enterasys.com:policy:p1# apcustom enable
EWC.enterasys.com:policy:p1#
```

20.5.11 apfilters

Use the **apfilters** command to enter the **policy:<named-policy>:apfilters** context for the configuring of AP custom filters. AP custom filters are applied at the AP. The **apfilters** command is accessible from the **policy:<named-policy>** context.

Notes: You must execute the **ulfilterap enable** command and the **apcustom enable** command before the **apfilters** command is visible.

The **apfilter** command has been replaced by **apfilters**. **apfilter** is deprecated.

The following commands are available in the **policy:<named-policy>:apfilters** context.

- create
- config
- delete
- move

Syntax

```
apfilter
```

Parameters

None.

Usage

The apply custom filters to AP feature must be enabled using the the **apcustom enable** command for the **apfilters** command to be visible in the CLI.

Examples

The following example enters the policy:<named-policy>:apfilters context for the **p1** <named-policy>:

```
EWC.enterasys.com:policy:p1# ulfilterap enable
EWC.enterasys.com:policy:p1# apcustom enable
EWC.enterasys.com:policy:p1# apfilters
EWC.enterasys.com:policy:p1:apfilters#
```

20.5.11.1 create

Use the **create** command to create, insert, or append a new AP custom filter for this <named-policy>. The **create** command is accessible from the **policy:<named-policy>:apfilters** context.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode syntax:

```
create <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|dst) out (none|src)
(allow | deny)
```

Advanced mode syntax:

```
create <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|src|dst|both) out
(none|src|dst|both) (allow | deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <protocol>	Specifies the protocol for this custom filter by number or name. Valid number values are from 0 - 255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **all** - All protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
<ipaddress/mask>	Specifies an IP address and mask for this custom filter.
interface-mask	Specifies that the IP address and mask configured for the associated topology will be used for this custom filter.
interface-ip	Specifies the IP address of the associated topology will be used for this custom filter.

port <port> [<port>]	Specifies a TCP or UDP port or port range to which this custom filter will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type <type> [<type>]	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0 - 255.
Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow. — **in** specifies a packet flow from the AP to the AC. **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
Basic: out (none|src) Advanced: out (none|src|dst|both)	Specifies the direction of packet flow. — **out** specifies a packet flow from the AC to the AP. **none** specifies that the **out** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
allow | deny	Specifies whether packets will be allowed or denied when meeting the criteria specified in the custom filter.

Usage

If the specified rule position already contains a custom filter, specifying a rule using this command inserts a rule in the currently existing rules position and moves all other rules by one position. Use the **create** command to insert or append a rule at the specified position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example creates a custom filter 1 that allows UDP traffic in both directions from IP address 10.10.10.0/24 for ports 10 through 2000:

```
EWC.enterasys.com:policy:p1:apfilters# create 1 proto udp 10.10.10.0/24 port 20
2000 in dst out src allow
EWC.enterasys.com:policy:p1:apfilters# apply
EWC.enterasys.com:policy:p1:apfilters# show
Custom AP Filters: enable
```

```
filter 1 proto udp 10.10.10.0 255.255.255.0 port 20 2000 in dst out src allow
filter 2 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 3 (default) proto none 0.0.0.0  all_ports in none out src allow
```

The following example creates a custom filter 1 that is inserted into the rule list at position 1 because a rule already exists for rule 1. This custom filter allows ICMP types 9 through 31 traffic in both directions from IP address 20.20.10.0/24:

```
EWC.enterasys.com:policy:p1:apfilters# create 1 proto icmp 20.20.10.0/24 type 9
31 in dst out src allow
EWC.enterasys.com:policy:p1:apfilters# show
Custom AP Filters: enable
filter 1 proto icmp 20.20.10.0 255.255.255.0 type 9 31 in dst out src allow
filter 2 proto udp 10.10.10.0 255.255.255.0 port 10 2000 in dst out src allow
filter 3 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0  all_ports in none out src allow
```

20.5.11.2 config

Use the **config** command to modify an existing AP custom filter for this <named-policy>. The **config** command is accessible from the **policy:<named-policy>:apfilters** context.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode syntax:

```
config <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|dst) out (none|src)
(allow|deny)
```

Advanced mode syntax:

```
config <pos> proto <protocol> (<ipaddress/mask> | interface-subnet | interface-ip)
[(port <port> [<port>]) | (type <type> [<type>])] in (none|src|dst|both) out
(none|src|dst|both) (allow|deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <protocol>	Specifies the protocol for this custom filter by number or name. Valid number values are from 0 - 255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **all** - All protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol

<ipaddress/mask>	Specifies an IP address and mask for this filter.
interface-subnet	Specifies the IP address and mask configured for the associated topology.
interface-ip	Specifies the IP address of the associated topology
port <port> [<port>]	Specifies a TCP or UDP port or port range to which this custom filter will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid Port values are from 0 - 65535.
type <type> [<type>]	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0 - 255.
Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow. — **in** specifies a packet flow from the AP to the AC. **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
Basic: out (none|src) Advanced: out (none|src|dst|both)	Specifies the direction of packet flow. — **out** specifies a packet flow from the AC to the AP. **none** specifies that the **out** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
allow | deny	Specifies whether packets will be allowed or denied when meeting the criteria specified in the custom filter.

Usage

If the specified rule position already contains a custom filter, this command overwrites the existing rule. Use the **create** command to insert or append a rule at the specified position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example overwrites a pre-existing custom filter 2 with a rule that allows TCP traffic both directions from IP address 50.20.0.0/16:

```
EWC.enterasys.com:vnsmode:default-policy:apfilters# config 2 proto tcp 50.20.0.0/
16 in dst out src allow
```

```
EWC.enterasys.com:vnsmode:default-policy:apfilters# show
Custom AP Filters: enable
filter 1 proto icmp 20.20.10.0 255.255.255.0 type 9 31 in dst out src allow
filter 2 proto tcp 50.20.0.0 255.255.0.0 all_ports in dst out src allow
filter 3 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0  all_ports in none out src allow
```

20.5.11.3 delete

Use the **delete** command to remove a custom filter from the AP filter list. The **delete** command is accessible from the **policy:<named-policy>:apfilters** context.

Syntax

```
delete <pos>
```

Parameters

<pos>	Specifies the custom filter list position of the filter to be deleted. Valid values are from 0 - 255.

Examples

The following example deletes custom filter 1 and displays the remaining default rules:

```
EWC.enterasys.com:policy:p1:apfilters# delete 1
EWC.enterasys.com:policy:p1:apfilters# show
Custom AP Filters: enable
filter 1 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 2 (default) proto none 0.0.0.0  all_ports in none out src allow
```

20.5.11.4 move

Use the **move** command to move a custom filter from its current position in the filter list to the specified filter list position. The **move** command is accessible from the **policy:<named-policy>:apfilters** context.

Syntax

```
move <cur-pos> <new-pos>
```

Parameters

<cur-pos> <new-pos>	Specifies the current position in the filter list of the rule to be moved, followed by the new list position for the custom filter. Valid values are from 0 - 255.

Examples

The following example:

- Moves the rule in list position 2 to list position 1

- Displays the new list ordering :

```
EWC.enterasys.com:policy:p1:apfilters# move 2 1
EWC.enterasys.com:policy:p1:apfilters# show
Custom AP Filters: enable
filter 1 proto tcp 50.20.0.0 255.255.0.0 all_ports both allow
filter 2 proto icmp 20.20.10.0 255.255.255.0 type 9 31 both allow
filter 3 (default) proto none 0.0.0.0  all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0  all_ports in none out src allow
```

21

topology Commands

This section describes commands used to define and configure topology objects used by policy and VNS objects. These commands are located in the **topology** context of the CLI. Execute the **topology** command at the root level to enter toplogy context.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

Note: The **topology** context was introduced with V7.11.

The following commands are available in the **topology** context:

- create
- delete
- <named-topology> — See <named-topology> for commands in the **topology:<named-topology>** context.
- show

21.1 create

Use the **create** command to create a Enterasys Wireless Controller topology object. The **create** command is accessible from the **topology** context of the CLI.

Syntax

```
create <topology name> b@ac <vlanid> port <port name>} |
b@ap <-1 | vlanid> | routed  <A.B.C.D/32>
```

Parameters

<topology name>	Specifies the name of the topology.
b@ac <vlanid> port <port name>	Specifies the VLAN ID and the port to which the VLAN is attached for a topology that is bridged locally at the controller.
b@ap <-1 | vlanid>	Specifies the VLAN Id for a topology that is bridged locally at the AP.
routed <A.B.C.D/32>	Specifies the IPv4 IP address and mask for a routed topology.

Usage

There are five topology types:

- Admin — The native, pre-defined topology of the Enterasys Wireless Controller management port. This topology is named admin. You cannot create topologies with the name admin.
- B@AC — Bridge Traffic Locally at controller. Requires Layer 2 configuration. May optionally have Layer 3 configuration. Layer 3 configuration would be necessary if services (such as DHCP) are required over the configured network segment, or if controller management operations are intended to be done through the configured interface.
- B@AP — Bridge Traffic Locally at AP. Requires Layer 2 configuration. Does not require Layer 3 configuration. Bridge Traffic at the AP topologies do not require the definition of a corresponding IP address since all traffic for users in that topology will be directly bridged by the Wireless AP at the local network point of attachment (VLAN at AP port).
- Routed — Routed topology. Routed topologies do not need any Layer 2 configuration, but do require Layer 3 configuration.
- Physical —Physical Ethernet port topology. Each Ethernet port has a pre-defined topology. The name of the topology matches the name of the port (for example, esa0). You cannot create topologies with the names of the physical Ethernet ports.

You can choose from only three of the topology types (modes) when creating a topology:

- B@AC
- B@AP
- Routed

Only topologies of these three types can be assigned to policies.

Examples

The following example creates a B@AC topology named bac1, with a VLAN ID of 2, using the esa1 controller port.

```
EWC.enterasys.com:topology# create bac1 b@ac 2 port esa1
```

21.2 delete

Use the **delete** command to delete a topology object. The **delete** command is accessible from the **topology** context of the CLI.

You cannot delete the Admin topology or a physical topology.

Note: You cannot delete a topology that is being used by a policy.

Syntax

```
delete <topology name>
```

Parameters

<topology name>	Specifies the name of the topology to delete

The following example deletes the topology named test.

```
EWC.enterasys.com:topology# delete test
```

21.3 show

Use the **show** command to display topology configuration information.

Syntax

show [<topology name>]

Parameters

<topology name>	Specifies to display information about the specific topology

Examples

The following example displays information for all configured topologies.

```
EWC.enterasys.com:topology# show

Name                    Mode      L2:VlanId,port  L3:IP,GW,


Admin                   admin     N/A,Admin       192.168.4.37,192.168.4.11,N/A
esa0                    physical  545,esa0        10.109.0.1,10.0.0.2,none
esa1                    physical  -1,esa1         10.0.1.1,10.0.1.2,none
Bridged at AP untagged  b@ap      -1,N/A
Enterasys-37Topology    b@ac      647,esa0        10.209.2.37,none,none
650                     b@ac      650,esa0
999                     b@ac      999,esa0
briAP                   b@ac      648,esa-1

Topology global info:
Internal VLAN ID: 1

Multicast support: disabled

EWC.enterasys.com:topology# show 650
Topology mode: b@ac
Synchronize: enable
Name: 650
Layer 3 presence: disable
```

The following example displays information for a physical topology named esa0.

```
EWC.enterasys.com:topology:esa0# show
Name: esa0
3rd party: disable
```

21.4 <named-topology>

The **<named-topology>** command, where <named-topology> refers to the name of a given topology, moves you into the **topology:<named-topology>** context, which contains commands to configure the settings of the specified individual topology.

The following commands are available in the **topology:<named-topology>** context.

- 3rd-party
- l2 — See l2 for commands in the **topology:<named-topology>:l2** context.
- l3 — See l3 for commands in the **topology:<named-topology>:l3** context.
- l3presence
- mode
- name
- show
- strict-subnet
- sync

21.4.1 3rd-party

Use the **3rd-party** command to enable or disable a third-party port in a physical topology. The **3rd-party** command is available from the **topology:<named-topology>** context of the CLI for physical topologies.

Note: Only one physical topology can have 3rd-party set to enable.

Syntax

```
3rd-party enable | disable
```

Parameters

enable	Enables a 3rd-party port on the specified physical topology.
disable	Disables a 3rd-party port on the specified physical topology.

Examples

The following example enables a 3rd-party port on a physical topology.

```
EWC.enterasys.com:topology:esa0# 3rd-party enable
EWC.enterasys.com:topology:esa0# show
Name: esa0
3rd party: enable
```

21.4.2 l2

Use the **l2** command to enter the **topology:<named-topology>:l2** context of the CLI for b@ac, b@ap, physical, and routed topologies. The l2 context allows you to configure the Layer 2 functionality of the topology.

The following commands are available in the **topology:<named-topology>:l2** context.

- multicast — See multicast for commands in the **topology:<named-topology>:l2:multicast** context.
- port
- show
- tagged
- vlanid

21.4.2.1 multicast

Use the **multicast** command to enter the **topology:<named-topology>:l2: multicast** context of the CLI for b@ac and routed topologies.

The following commands are available in the **topology:<named-topology>:l2: multicast** context.

- config
- create
- delete
- filter
- move

21.4.2.1.1 config

Use the **config** command to configure an existing multicast filter. The **config** command is available from the **topology:<named-topology>:l2:multicast** context of the CLI for b@ac and routed topologies.

Note: To create a multicast filter, use the **create** command. See “create” on page 21-6.

Syntax

```
config <pos>|default (A.B.C.D[/<0-32>] | vocera | svp) on|off
```

Parameters

<pos>|default	Specifies the priority of filter rule (0–255) or default filter rule.
A.B.C.D[/<0-32>] | vocera | svp	Specifies the IP address and mask of a multicast group or that the multicast group is pre-defined. • svp: Spectralink SVP (224.0.1.116) • vocera: Vocera Mcst (230.230.0.0/20)
on|off	Specifies whether wireless replication is enabled. The default is off.

Examples

This example configures an existing multicast filter.

```
EWC.enterasys.com:topology:techpubs_test_ac:l2:multicast# config 1 225.1.1.0/32
on
```

21.4.2.1.2 create

Use the **create** command to create a multicast filter rule. The **create** command is available from the **topology:<named-topology>:l2:multicast** context of the CLI for b@ac and routed topologies.

Syntax

```
create [<pos>|default] (A.B.C.D[/<0-32>] | vocera | svp) on|off
```

Parameters

<pos>|default	Specifies the optional position of the rule, or whether the rule is the default rule.
A.B.C.D[/<0-32>] | vocera | svp	Specifies the IP address and mask of a multicast group or that the multicast group is pre-defined. • svp: Spectralink SVP (224.0.1.116) • vocera: Vocera Mcst (230.230.0.0/20)
on|off	Specifies whether wireless replication is enabled. The default is off.

Examples

This example creates a multicast filter rule.

```
EWC.enterasys.com:topology:techpubs_test_ac:l2:multicast# create 1 225.1.1.0/32
on
```

21.4.2.1.3 delete

Use the **delete** command to delete a multicast filter rule. The **delete** command is available from the **topology:<named-topology>:l2:multicast** context of the CLI for b@ac and routed topologies.

Syntax

```
delete <pos>
```

Parameters

<pos>	The position of the multicast filter rule.

Examples

This example deletes a multicast filter rule.

```
EWC.enterasys.com:topology:test:l2:multicast# delete 2
```

21.4.2.1.4 filter

Use the **filter** command to enable or disable multicast filtering support. The **filter** command is available from the **topology:<named-topology>:l2:multicast** context of the CLI for b@ac and routed topologies.

Syntax

```
filter enable | disable
```

Parameters

enable	Indicates that multicast filtering support will be enabled.
disable	Indicates that multicast filtering support will be disabled.

Examples

This example enables multicast filtering support.

```
EWC.enterasys.com:topology:test:l2:multicast# filter enable
```

21.4.2.1.5 move

Use the **move** command to change the order of multicast rules. The **move** command is available from the **topology:<named-topology>:l2:multicast** context of the CLI for b@ac and routed topologies.

Syntax

```
move <pos> <pos>
```

Parameters

<pos>	The current position of the multicast rule. Possible values are 0–255.
<pos>	The new position of the multicast rule. Use a number one greater than the last rule to move a rule to the bottom of the list. Possible values are 0–255.

Examples

This example moves multicast rule 2 to the bottom of the list.

```
EWC.enterasys.com:topology:test:l2:multicast# move 2 5
```

21.4.2.1.6 show

Use the **show** command to show multicast support for the specified topology. The **show** command is available from the **topology:<named-topology>:l2: multicast** context of the CLI for b@ac and routed topologies.

Syntax

```
show
```

Parameters

None

Examples

This example shows the multicast support for a topology named r1.

```
EWC.enterasys.com:topology:r1:l2:multicast# show
Multicast support: disable
```

21.4.2.2 port

Use the **port** command to assign a port to a topology. The **port** command is available from the **topology:<named-topology>:l2** context of the CLI for b@ac topologies.

Syntax

```
port <port name>
```

Parameters

<port name>	Specifies the name of the port

Examples

This example assigns port esa1 to the topology named r1.

```
EWC.enterasys.com:topology:r1:l2:port# port esa1
```

21.4.2.3 show

Use the **show** command to show layer 2 information about the specified topology. The **show** command is available from the **topology:<named-topology>:l2** context of the CLI for b@ac, b@ap, and routed topologies

Syntax

```
show
```

Parameters

None

Examples

This example shows layer 2 information for a b@ac topology named briAC_test.

```
EWC.enterasys.com:topology:briAC_test:l2# show
Port: esa0
VLAN ID: 333
Foreign Port: esa0
```

21.4.2.4 tagged

Use the **tagged** command to enable or disable 802.1Q VLAN tagging. The **tagged** command is available from the **topology:<named-topology>:l2** context of the CLI for b@ap and physical topologies.

Syntax

```
tagged enable | disable
```

Parameters

enable	Indicates that 802.1Q VLAN tagging will be enabled.
disable	Indicates that 802.1Q VLAN tagging will be disabled.

Examples

This following example enables 802.1Q VLAN tagging on the physical topology named esa1.

```
EWC.enterasys.com:topology:esa1:l2# tagged enable
```

21.4.2.5 vlanid

Use the **vlanid** command to configure the VLAN ID of a physical topology or change the VLAN ID of b@ac or b@ap topologies. The **vlanid** command is available from the **topology:<named-topology>:l2** context of the CLI for b@ac, b@ap, and physical topologies.

Syntax

```
vlanid <1-4094>
```

Parameters

<1-4094>	The VLAN ID that you want to assign to the topology.

Examples

This following example sets the VLAN ID of the topology named test to 2.

```
EWC.enterasys.com:topology:test:l2# vlanid 2
```

21.4.3 l3

Use the **l3** command to enter the **topology:<named-topology>:l3** context of the CLI for admin, b@ac, physical, and routed topologies. The l3 context allows you to configure the Layer 3 functionality of the topology. The l3 context is available in b@ac mode only if **l3presence** is set to **enable**. For more information, see "l3presence" on page 21-30.

The following commands are available in the **topology:<named-topology>:l3** context.

- ap-register
- cert
- copy-csr
- dhcp — See dhcp for commands in the **topology:<named-topology>:l3: dhcp** context.

- exceptions — See exceptions for commands in the **topology:<named-topology>:l3:exceptions** context.
- foreign-ip
- gateway
- gen-certreq
- ip
- mgmt
- mtu
- nexthop
- ospf-advert
- ospf-cost
- show

21.4.3.1 ap-register

Use the **ap-register** command to enable or disable AP registration through the named topology. The **ap-register** command is available from the **topology:<named-topology>:l3** context of the CLI for b@ac and physical topologies.

Syntax

```
ap-register enable | disable
```

Parameters

enable	Enables AP registration through this interface.
disable	Disables AP registration through this interface.

Examples

The following example enables AP registration.

```
EWC.enterasys.com:topology:esa0:l3# ap-register enable
```

21.4.3.2 cert

Use the **cert** command to define certificate settings for the named topology in the current context.

Using the **cert** command with the default option removes the certificate from the named topology and assigns the factory default certificate to it.

Syntax

```
cert (( pkcs12 <scp|ftp> <server> <user> <password> <dir> <filename>
<certpassword> [chainfile]) | (pem-der <scp|ftp> <server> <user> <password> <dir>
<filename> <keyfile> <certpassword> [chainfile])| (csr-cert <scp|ftp> <server>
<user> <password> <dir> <filename> [chainfile])) | permanent | permanent-chain |
default
```

Parameters

pkcs12	Indicates that <*filename*> certificate file is in the PKCS #12 format.
pem-der	Indicates that the <*filename*> certificate file and <keyfile> key file are PEM/DER encoded.
csr-cert	Indicates that the <*filename*> is a certificate signing request file.
<**scp**|**ftp**>	Indicates that either SCP or FTP should be used to download the certificate file.
<*server*>	IP address of the server from which the file should be downloaded
<*user*>	Userid of the account to login with on the SCP or FTP server
<*password*>	Password associated with the <user> userid
<*dir*>	Directory in which to find the PKCS #12 certificate file, CSR file, or PEM/DER encoded certificate file and key file.
<*filename*>	The name of the PKCS #12, PEM/DER, or CSR certificate file to use with the port. This must be a PKCS #12 file if the permanent option is not used.
<*keyfile*>	The PEM/DER encoded private key file
<*certpassword*>	Password to use with the private key file
[*chainfile*]	A PEM-formatted CA (Certification Authority) chain certificate file. If you choose to install this optional certificate, you must do so when specifying the PCKCS #12 or PEM/DER certificates.
permanent	Indicates that the certificate to use is already in the permanent key store. This is used by the export and show commands to show which certificate is assigned to each port. The certificate will then be applied to the wireless assistant virtual website bound to the port the context of which the command was issued in.
permanent-chain	Indicates that the chain certificate to use is already in the permanent key store. This is used by the export and show commands to show which certificate is assigned to each port. The certificate will then be applied to the wireless assistant virtual website bound to the port the context of which the command was issued in.
default	Indicates that the interface should use the factory default certificate and key.

Usage

Use the **cert** command to define certificate settings for the named topology in the current context. With the **cert** command, you can either to assign a downloaded PKCS #12 file, CSR file, or PEM/DER files to the named topology or to reset the named topology to use the factory default certificate.The **cert** command is available from the **topology:<named-topology>:l3** context of the CLI for admin, b@ac, physical, and routed topologies.

When you use the **cert** command to assign a PKCS #12 file, CSR file, or PEM/DER files to an interface, you must select either SCP or FTP as the file transfer mechanism and specify the PKCS#12 file, CSR file, or PEM/DER files. The command then attempts to download the specified

PKCS#12 file, CSR file, or PEM/DER files, and, if successful, converts the PKCS#12 file, CSR file, or PEM/DER files into a certificate and key. The command confirms that the certificate password works with the private key file then assigns both the certificate and key to the named topology.

Note: This command generates an error if the indicated file name cannot be found.

Using the **cert** command with the default option removes the certificate from the named topology and assigns the factory default certificate to it.

Examples

The following example downloads a PKCS #12 certificate file and a chain certificate using FTP and applies it to the topology named test.

```
EWC.enterasys.com:topology:test:l3# cert pkcs12 ftp 1.1.1.1 test abc123 /test
test.pfx abc123 chain.crt
Attempting to download file using ftp ...
```

The following example downloads a PEM/DER certificate file, a PEM/DER key file, and a chain certificate using FTP and applies it to the topology named test.

```
EWC.enterasys.com:topology:test:l3# cert per-der ftp 1.1.1.1 test abc123 /test
t certificate.crt privatekey.key abc123 chain.crt
Attempting to download file using ftp ...
```

The following example downloads a CSR file using FTP and applies it to the topology named test.

```
EWC.enterasys.com:topology:test:l3# cert csr-cert ftp 1.1.1.1 test abc123 /test
test.csr
```

The following example sets the certificate to the factory default for the topology named test.

```
EWC.enterasys.com:topology:test:l3# cert default
EWC.enterasys.com:topology:test:l3# show cert
Factory default certificate/key
```

21.4.3.3 copy-csr

Use this command to upload a topology certificate signing request to a server. The **copy-scr** command is available in the **topology:<named-topology>:l3** context.

Syntax

```
copy-csr <scp|ftp> <server> <user> <password> <dir>
```

Parameters

scp | **ftp**	Specifies the type of server, FTP or SCP, to which the file will be uploaded.
server	IP address of the FTP or SCP server.
user	User name to login to the server.
password	User password.
dir	Directory on server to put the certificate signing request file.

Examples

```
EWC.enterasys.com:topology:test:l3# copy-csr ftp 192.168.1.1 root mypasswd /tmp
```

21.4.3.4 dhcp

Use the **dhcp** command to enter the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies.

The following commands are available in the **topology:<named-topology>:l3: dhcp** context.

- dhcp-servers
- dls
- dls-address
- dns
- domain
- exclude
- foreign-gateway
- foreign-range
- gateway
- lease-default
- lease-max
- mode
- range
- show
- wins

21.4.3.4.1 dhcp-servers

Use the **dhcp-servers** command to configure DHCP relay servers. The **dhcp-servers** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac and routed topologies. This command is visible only when **mode** is set to **relay**. See "mode" on page 21-18.

Syntax

```
dhcp-servers (A.B.C.D [,A.B.C.D [...]]) | none
```

Parameters

A.B.C.D [,A.B.C.D [...]]	Specifies qualified IPv4 address of DHCP relay servers
none	Clears DHCP relay servers

Examples

The following example sets the IP address of the DHCP relay server as 10.0.1.10.

```
EWC.enterasys.com:topology:test:l3:dhcp# mode relay
EWC.enterasys.com:topology:test:l3:dhcp# dhcp-servers 10.0.1.10
```

21.4.3.4.2 dls

Use the **dls** command to enable or disable DLS (HiPath Deployment Services). The **dls** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
dls enable | disable
```

Parameters

enable	Enables DLS
disable	Disables DLS

Examples

The following example enables DLS.

```
EWC.enterasys.com:topology:test:l3:dhcp# mode local
EWC.enterasys.com:topology:test:l3:dhcp# dls enable
```

The following example disables DLS.

```
EWC.enterasys.com:topology:test:l3:dhcp# mode local
EWC.enterasys.com:topology:test:l3:dhcp# dls disable
```

Note: After you run the **dls** command, you must run the **apply** command to implement the changes.

21.4.3.4.3 dls-address

Use the **dls-address** command to configure the DLS server address and port. The **dls-address** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac and routed topologies. This command is visible only when **mode** is set to **local** and **dls** is set to **enable**. See "mode" on page 21-18.

Syntax

```
dls-address (A.B.C.D | name) port <0-65535>
```

Parameters

A.B.C.D | name	Specifies the qualified IPv4 address or name
port <0-65535>	Specifies the DLS port number. This is an optional parameter. The default port is 18433.

Examples

The following example sets the DLS address as 10.10.0.10.

```
EWC.enterasys.com:topology:test:l3:dhcp# mode local
EWC.enterasys.com:topology:test:l3:dhcp# dls enable
EWC.enterasys.com:topology:test:l3:dhcp# dls-address 10.10.0.10
```

21.4.3.4.4 dns

Use the **dns** command to specify the IP addresses for one or more DNS servers. The **dns** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
dns (<DNS server> [,<DNS server> [...]]) | none
```

Parameters

<DNS server>	Specifies the IP address of a DNS server
none	Clears the DNS server

Examples

The following example specifies the IP addresses of two DNS servers.

```
EWC.enterasys.com:topology:test:l3:dhcp# mode local
EWC.enterasys.com:topology:test:l3:dhcp# dns 192.168.1.2, 192.168.1.3
EWC.enterasys.com:topology:test:l3:dhcp# apply
```

Note: After you run the **dns** command, you must run the **apply** command to implement the changes.

21.4.3.4.5 domain

Use the **domain** command to configure a domain name. The **domain** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
domain <domain name> | none
```

Parameters

<domain name>	Specifies the domain name or an IPv4 address.
none	Clears the domain name.

Examples

The following example sets the domain name as my-domain.

```
EWC.enterasys.com:topology:test:l3:dhcp# mode local
EWC.enterasys.com:topology:test:l3:dhcp# domain my-domain
```

21.4.3.4.6 exclude

Use the **exclude** command to exclude an IP address or a range of IP addresses from the DHCP Address Range. The **exclude** command is available from the **topology:<named-topology>:l3:dhcp**

context of the CLI for b@ac, physical, and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
exclude A.B.C.D [A.B.C.D] [delete | (comment <comment string>)]
```

Parameters

A.B.C.D[A.B.C.D]	Specifies the IP address or range of IP addresses.
delete	Clears the IP addresses.
comment <comment string>	A comment about the excluded IP address or range of IP addresses.

Examples

The following example excludes the address range 10.0.1.10–10.0.1.20.

```
EWC.enterasys.com:topology:test:l3:dhcp# mode local
EWC.enterasys.com:topology:test:l3:dhcp# exclude  10.0.1.10 10.0.1.20
```

21.4.3.4.7 foreign-gateway

Use the **foreign-gateway** command to configure the remote Enterasys Wireless Controller in a paired controller configuration. The **foreign-gateway** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
foreign-gateway A.B.C.D | none
```

Parameters

A.B.C.D	Specifies the IP address of the remote Enterasys Wireless Controller.
none	Clears the IP address of the remote Enterasys Wireless Controller.

Examples

The following example clears the IP address of the remote Enterasys Wireless Controller.

```
EWC.enterasys.com:topology:routed1:l3:dhcp# mode local
EWC.enterasys.com:topology:routed1:l3:dhcp# foreign-gateway none
```

21.4.3.4.8 foreign-range

Use the **foreign-range** command to configure the DHCP pool of addresses for a remote Enterasys Wireless Controller in a paired controller configuration. The **foreign-range** command is available

from the **topology:<named-topology>:l3: dhcp** context of the CLI for b@ac and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
foreign-range A.B.C.D A.B.C.D
```

Parameters

A.B.C.D	Specifies the first IP address in the IP address range
A.B.C.D	Specifies the last IP address in the IP address range

Examples

The following example specifies the IP address range.

```
EWC.enterasys.com:topology:routed2:l3:dhcp# mode local
EWC.enterasys.com:topology:routed2:l3:dhcp# foreign-range 10.44.6.2 10.44.6.254
```

21.4.3.4.9 gateway

Use the **gateway** command to specify the gateway IP address. The **gateway** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac and physical topologies. For information about the **gateway** command for the admin topology, see "gateway" on page 21-26.

Syntax

```
gateway A.B.C.D | none
```

Parameters

A.B.C.D	Specifies the gateway IP address.
none	Clears the gateway IP address.

Examples

The following example clears the gateway IP address.

```
EWC.enterasys.com:topology:esa1:l3:dhcp# gateway none
```

21.4.3.4.10 lease-default

Use the **lease-default** command to set the default time limit, in seconds, that an IP address would be assigned by the DHCP server to a wireless device. The **lease-default** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
lease-default <int>
```

Parameters

<int>	Specifies the time limit in seconds

Examples

The following example sets the default lease time to 34000 seconds.

```
EWC.enterasys.com:topology:routed2:l3:dhcp# mode local
EWC.enterasys.com:topology:routed2:l3:dhcp# lease 34000
EWC.enterasys.com:topology:routed2:l3:dhcp# apply
```

Note: After you run the **lease-default** command, you must run the **apply** command to implement the changes.

21.4.3.4.11 lease-max

Use the **lease-max** command to set the maximum time limit, in seconds, that an IP address would be assigned by the DHCP server to a wireless device. The **lease-max** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
lease-max <int>
```

Parameters

<int>	Specifies the time limit in seconds

Examples

The following example sets the maximum time to keep a DHCP-assigned IP address to 2592000 seconds.

```
EWC.enterasys.com:topology:routed2:l3:dhcp# mode local
EWC.enterasys.com:topology:routed2:l3:dhcp# lease-max 2592000
EWC.enterasys.com:topology:routed2:l3:dhcp# apply
```

Note: After you run the **lease-max** command, you must run the **apply** command to implement the changes.

21.4.3.4.12 mode

Use the **mode** command to specify the type of DHCP server to be used. The **mode** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies.

Syntax

- For b@ac topologies: `mode local | relay | none`
- For physical topologies: `mode local | none`
- For routed topologies: `mode local | relay`

Parameters

local	Indicates that the controller itself acts as the DHCP server

relay	Indicates that a DHCP relay server will be used
none	Indicates that the Enterasys Wireless Controller will not treat the DHCP messages specially

Examples

The following example configures the routed topology named routed2 to use a local DHCP server on the controller.

```
EWC.enterasys.com:topology:routed2:l3:dhcp# mode local
EWC.enterasys.com:topology:routed2:l3:dhcp# apply
```

Note: After you run the **mode** command, you must run the **apply** command to implement the changes.

21.4.3.4.13 range

Use the **range** command to configure the DHCP pool of addresses. The **range** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
range A.B.C.D A.B.C.D
```

Parameters

A.B.C.D	Specifies the first IP address in the IP address range
A.B.C.D	Specifies the last IP address in the IP address range

Examples

The following example defines the DHCP range of IP addresses.

```
EWC.enterasys.com:topology:routed2:l3:dhcp# mode local
EWC.enterasys.com:topology:routed2:l3:dhcp# range 192.168.1.30 192.168.1.54
EWC.enterasys.com:topology:routed2:l3:dhcp# apply
```

Note: After you run the **range** command, you must run the **apply** command to implement the changes.

21.4.3.4.14 show

Use the **show** command to display DHCP information for the specified topology. The **show** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies.

The output of the **show** command is determined by how **mode** is set. See "mode" on page 21-18.

Syntax

```
show
```

Parameters

None

Examples

The following example shows DHCP information for a physical topology with **mode** set to **local**:

```
EWC.enterasys.com:topology:esa1:l3:dhcp# show
DHCP option: local
Gateway: 10.0.1.2
Address range: 10.109.1.2 10.109.1.254
exclude 10.109.1.5(interface address)
DNS servers:
Domain name:
Max lease time: 2592000
Default lease time: 36000
WINS servers:
```

21.4.3.4.15 wins

Use the **wins** command to specify the IP address for the Windows Internet Naming Service (WINS) server. The **wins** command is available from the **topology:<named-topology>:l3:dhcp** context of the CLI for b@ac, physical, and routed topologies. This command is visible only when **mode** is set to **local**. See "mode" on page 21-18.

Syntax

```
wins (<WINS server> [,<WINS server> [...]]) | none
```

Parameters

<WINS server> [,<WINS server> [...]]	Specifies the qualified IPv4 IP address or name of one or more WINS servers.
none	Clears the IP addresses and indicates that no WINS server is present.

Examples

The following example specifies the IP addresses of two WINS servers.

```
EWC.enterasys.com:topology:r1:l3:dhcp# mode local
EWC.enterasys.com:topology:r1:l3:dhcp# wins 192.168.1.3, 192.168.1.4
EWC.enterasys.com:topology:r1:l3:dhcp# apply
```

Note: After you run the **wins** command, you must run the **apply** command to implement the changes.

21.4.3.5 exceptions

Use the **exceptions** command to enter the **topology:<named-topology>:l3: exceptions** context of the CLI for b@ac, physical, and routed topologies. In this context, you can configure exception filters.

Note: The **exception** command has been replaced by the **exceptions** command. **exception** is deprecated.

The following commands are available in the **topology:<named-topology>:l3: exceptions** context.

- config
- create
- delete
- move
- show

21.4.3.5.1 config

Use the **config** command to configure an existing exception filter. The **config** command is available from the **topology:<named-topology>:l3:exceptions** context of the CLI for b@ac, physical, and routed topologies.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Note: To create an exception filter, use the **create** command. See “create” on page 21-23.

Syntax

Basic mode syntax:

```
config <pos> proto {udp|tcp|ah|esp|none|icmp|gre|<0-255>} A.B.C.D/<0-32> [(port
<0-65535>[ <0-65535>])|(type <0-255> [<0-255>])] in (dst|none) (allow|deny)
```

Advanced mode syntax:

```
config <pos> proto {udp|tcp|ah|esp|none|icmp|gre|<0-255>} A.B.C.D/<0-32> [(port
<0-65535>[ <0-65535>])|(type <0-255> [<0-255>])] in (none|src|dst|both)
(allow|deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0–255.

proto {udp|tcp|ah|esp|none|icmp|gre|<0-255>}	Specifies the protocol for this filter rule by number or name. Valid number values are from 0–255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **none** - No protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
A.B.C.D/<0-32>	Specifies the IPv4 IP address and mask.
(port <0-65535>[<0-65535>])	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a port range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0–65535.
(type <0-255> [<0-255>])	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0–255.
Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow — **in** specifies a packet flow from the AP to the AC. **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
(allow|deny)	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified exception filter position already contains an exception filter, the **config** command overwrites the existing exception filter. Use the **create** command to insert or append an exception filter at the specified position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example modifies an existing filter.

```
EWC.enterasys.com:topology:r1:l3:exceptions# config 2 proto tcp 1.1.1.1/32 port
80 in dst allow
```

21.4.3.5.2 create

Use the **create** command to create an exception filter. The **create** command is available from the **topology:<named-topology>:l3:exception** context of the CLI for b@ac, physical, and routed topologies.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Syntax

Basic mode syntax:

```
create [<pos>] proto {udp|tcp|ah|esp|none|icmp|gre|<0-255>} A.B.C.D/<0-32> [(port
<0-65535>[ <0-65535>])|(type <0-255> [<0-255>])] in(none|dst) (allow|deny)
```

Advanced mode syntax:

```
create [<pos>] proto {udp|tcp|ah|esp|none|icmp|gre|<0-255>} A.B.C.D/<0-32> [(port
<0-65535>[ <0-65535>])|(type <0-255> [<0-255>])] in(none|src|dst|both)
(allow|deny)
```

Parameters

<pos>	Specifies a position value for this filter in the filter list. Valid values are from 0–255.
proto {udp|tcp|ah|esp|none|icmp|gre|<0-255>}	Specifies the protocol for this filter rule by number or name. Valid number values are from 0–255. Valid name values are: • **udp** - UDP protocol • **tcp** - TCP protocol • **ah** - Authentication Header protocol • **esp** - Encapsulating Security Payload protocol • **none** - No protocols • **icmp** - ICMP protocol • **gre** - Generic Route Encapsulation protocol
A.B.C.D/<0-32>	Specifies the IPv4 IP address and mask.
(port <0-65535>[<0-65535>])	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a port range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0–65535.
(type <0-255> [<0-255>])	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0–255.

Basic: in (none|dst) Advanced: in (none|src|dst|both)	Specifies the direction of packet flow — **in** specifies a packet flow from the AP to the AC. **none** specifies that the **in** direction does not apply to the filter rule. **dst** specifies that the IP address for this filter rule is the destination of the packet flow. **src** specifies that the IP address for this filter rule is the source of the packet flow. **both** specifies that the IP address for this filter rule can be either source or destination.
(allow|deny)	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified exception filter position already contains an exception filter, specifying an exception filter using this command inserts the exception filter in the specified position in the list and resequences all filters below this filter down by one position. Use the **create** command to insert or append a rule at the specified position.

If advanced filter mode has been enabled with the enable-advance-filtering command (page 20-3), the Advanced mode syntax is presented. If advanced filter mode is not enabled, the Basic mode syntax is presented.

Examples

The following example creates an exception filter.

```
EWC.enterasys.com:topology:r1:l3:exceptions# create 2 proto tcp 1.1.1.1/32 port
80 in dst deny
```

21.4.3.5.3 delete

Use the **delete** command to delete an exception filter. The **delete** command is available from the **topology:<named-topology>:l3:exceptions** context of the CLI for b@ac, physical, and routed topologies.

Syntax

```
delete <pos>
```

Parameters

<pos>	Specifies the position of the exception filter (0–255).

Examples

The following example deletes the exception filter at position 2.

```
EWC.enterasys.com:topology:r1:l3:exceptions# delete 2
```

21.4.3.5.4 move

Use the **move** command to change the order (position) of an exception filter. The **move** command is available from the **topology:<named-topology>:l3: exceptions** context of the CLI for b@ac, physical, and routed topologies.

Syntax

```
move <pos> <pos>
```

Parameters

<pos>	Specifies the current position of the exception filter (0–255).
<pos>	Specifies the new position of the exception filter (0–255).

Examples

The following example moves exception filter at position 4 to 25.

```
EWC.enterasys.com:topology:r1:l3:exceptions# move 4 25
```

21.4.3.5.5 show

Use the **show** command to display a list of exception filters. The **show** command is available from the **topology:<named-topology>:l3:exceptions** context of the CLI for b@ac, physical, and routed topologies.

Syntax

```
show
```

Parameters

None

Examples

The following example displays the exception filters for the r1 topology.

```
EWC.enterasys.com:topology:r1:l3:exceptions# show
Exception filter(I): 1027 proto tcp 11.11.11.17 255.255.255.255 port 60606 both deny
Exception filter(I): 1028 proto tcp 0.0.0.0 255.255.255.255 port 50200 both deny
Exception filter(I): 1029 proto tcp 11.11.11.17 255.255.255.255 port 32768 65535 both
allow
Exception filter(I): 1030 proto udp 11.11.11.17 255.255.255.255 port 32768 65535 both
allow
Exception filter(I): 1031 proto udp 11.11.11.17 255.255.255.255 port 67 both allow
Exception filter(I): 1032 proto udp 255.255.255.255 255.255.255.255 port 67 both allow
Exception filter(I): 1033 proto icmp 11.11.11.17 255.255.255.255 port 0 255 both allow
Exception filter(I): 1034 proto none 0.0.0.0   both deny
```

Note: In the **show** command output, the (I) indicates that the exception filter is an internal (read-only) filter that has been pre-defined.

21.4.3.6 foreign-ip

Use the **foreign-ip** command to specify the IP address and subnet mask of the foreign controller. The **foreign-ip** command is available from the **topology:<named-topology>:l3** context of the CLI for b@ac and routed topologies.

Syntax

```
foreign-ip A.B.C.D/<0-32>
```

Parameters

A.B.C.D/<0-32>	Specifies the IP address and subnet mask.

Examples

The following example specifies the IP address and mask of the foreign controller.

```
EWC.enterasys.com:topology:r1:l3:# foreign-ip
```

21.4.3.7 gateway

Use the **gateway** command to specify the gateway IP address. The **gateway** command is available from the **topology:<named-topology>:l3** context of the CLI for the admin topology.

Syntax

```
gateway A.B.C.D | none
```

Parameters

A.B.C.D	Specifies the gateway IP address.
none	Clears the gateway IP address.

Examples

The following example clears the gateway IP address.

```
EWC.enterasys.com:topology:admin:l3:# gateway none
```

21.4.3.8 gen-certreq

Use this command to generate a certificate signing request and private key for the named topology. The **gen-certreq** command is available from the **topology:<named-topology>:l3** context of the CLI.

Syntax

```
gen-certreq <cn> [(location <country> <state> <city>) (organization <name> <unit>)
(email <email-address>)]
```

Parameters

cn	Common name that you want to assign to the controller interfaces. This is a mandatory parameter.

location	Keyword indicating that the next three parameters specify the location where the controller is operating.
country	The name of the country where the controller is located. You must use the two-letter ISO abbreviation for the country.
state	The name of the state or province where the controller is located
city	The name of the city where the controller is located
organization	Keyword indicating that the next two parameters specify the name of the organization to which the controller belongs.
name	Organization name.
unit	Organization unit name.
email	Key word that identifies the following parameter as an email address.
email_addr	Email address.

Usage

If a DNS name is used as the common name, a DNS lookup is performed. If the DNS name is not found, a warning is displayed.

Once the CSR file has been created, you can copy it to an FTP or SCP server using the copy-csr command (page 21-12). You can apply the certificate with the cert command (page 21-10).

Examples

```
EWC.enterasys.com:ap:topology:Seg1_Routed:l3# gen_certreq seg1_routed location CA
Ontario Mississauga organization mnj_Ware_House Service email me@email.com
```

21.4.3.9 ip

Use the **ip** command to specify the Enterasys Wireless Controller IP address and subnet mask for physical and routed topologies or the interface IP address and subnet mask for b@ac topologies. The **ip** command is available from the **topology:<named-topology>:l3** context of the CLI for admin, b@ac, physical, and routed topologies.

Syntax

```
ip A.B.C.D/<0-32>
```

Parameters

A.B.C.D/<0-32>	Specifies the IP address and subnet mask.

Examples

The following example specifies the IP address and subnet mask.

```
EWC.enterasys.com:topology:r1:l3:# ip 10.109.0.1/32
```

21.4.3.10 mgmt

Use the **mgmt** command to allow or prohibit management traffic. The **mgmt** command is available from the **topology:<named-topology>:l3** context of the CLI for b@ac, physical, and routed topologies.

Syntax

```
mgmt enable | disable
```

Parameters

enable	Enables management traffic.
disable	Disable management traffic.

Examples

The following example enables management traffic.

```
EWC.enterasys.com:topology:r1:l3:# mgmt enable
```

21.4.3.11 mtu

Use the **mtu** command to set the interface MTU (Maximum Transmission Unit), which specifies the maximum allowable size, in bytes, of a data packet on the Ethernet port. The **mtu** command is available from the **topology:<named-topology>:l3** context of the CLI for admin, b@ac, physical, and routed topologies.

Syntax

```
mtu <576-1500>
```

Parameters

<576-1500>	Specifies the size, in bytes, of the MTU.

Examples

The following example sets the size of the MTU to 1500 bytes.

```
EWC.enterasys.com:topology:r1:l3:# mtu 1500
```

21.4.3.12 nexthop

Use the **nexthop** command to set the IP address of the next hop router through which traffic will be directed. The **nexthop** command is available from the **topology:<named-topology>:l3** context of the CLI for routed topologies.

Syntax

```
nexthop A.B.C.D | none
```

Parameters

A.B.C.D	Specifies the IP address of the next hop router.
none	Clears the IP address of the next hop router.

Examples

The following example sets the IP address of the next hop router (169.232.75.1).

```
EWC.enterasys.com:topology:r1:l3:# nexthop 169.232.75.1
```

Note: After you run the **nexthop** command, you must run the **apply** command to implement the changes.

21.4.3.13 ospf-advert

Use the **ospf-advert** command to enable or disable OSPF advertisements on the topology. The **ospf-advert** command is available from the **topology:<named-topology>:l3** context of the CLI for routed topologies.

Syntax

```
ospf-advert enable | disable
```

Parameters

enable	Enables OSPF advertisements.
disable	Disables OSPF advertisements.

Examples

The following example enables OSPF advertisements.

```
EWC.enterasys.com:topology:r1:l3:# ospf-advert enable
```

Note: After you run the **ospf-advert** command, you must run the **apply** command to implement the changes.

21.4.3.14 ospf-cost

Use the **ospf-cost** command to set the OSPF route cost value. The **ospf-cost** command is available from the **topology:<named-topology>:l3** context of the CLI for routed topologies.

Syntax

```
ospf-cost <1-50000>
```

Parameters

<1-50000>	Specifies the OSPF route cost value.

Examples

The following example sets the OSPF route cost value to 6000

```
EWC.enterasys.com:topology:r1:l3:# ospf-cost 6000
```

Note: After you run the **ospf-cost** command, you must run the **apply** command to implement the changes.

21.4.3.15 show

Use the **show** command to display Layer 3 information. The **show** command is available from the **topology:<named-topology>:l3** context of the CLI for admin, b@ac, physical, and routed topologies.

Syntax

```
show
```

Parameters

None

Examples

The following example displays Layer 3 information for a physical topology.

```
EWC.enterasys.com:topology:esa0:l3# show
Interface IP 10.109.0.1 255.255.255.0
AP Registration: enable
Allow management traffic: disable
Factory default certificate/key
MTU: 1500
```

The following example displays Layer 3 information for a b@ac topology.

```
EWC.enterasys.com:topology:bridged_ac1:l3# show
Interface IP 0.0.0.0 0.0.0.0
AP Registration: disable
Allow management traffic: disable
Factory default certificate/key
Strict Subnet Adherence: enable
MTU: 1436
```

21.4.4 l3presence

Use the **l3presence** command to enable or disable Layer 3 on a b@ac topology. The **l3presence** command is available from the **topology:<named-topology>** context of the CLI for b@ac topologies.

Note: You must enable Layer 3 on a b@ac topology to access Layer 3 commands in the **topology:<named-topology>:l3** context.

Syntax

```
l3presence enable | disable
```

Parameters

enable	Enables Layer 3.

disable	Disables Layer 3.

Examples

The following example enables Layer 3 on a b@ac topology.

```
EWC.enterasys.com:topology:bridged_ac1# l3presence enable
```

21.4.5 mode

Use the **mode** command to change the mode of an existing b@ac, b@ap, or routed topology. The **mode** command is available from the **topology:<named-topology>** context of the CLI for b@ac, b@ap, and routed topologies.

Note: You can configure the mode of a topology only if the topology is not associated with a policy.

Syntax

```
mode b@ap | b@ac | routed
```

Parameters

b@ap | b@ac | routed	Specifies the mode of the topology.

Examples

The following example changes the mode of the topology to b@ap.

```
EWC.enterasys.com:topology:bridged_ac1# mode b@ap
```

21.4.6 name

Use the **name** command to change the name of an existing b@ac, b@ap, or routed topology. The **name** command is available from the **topology:<named-topology>** context of the CLI for b@ac, b@ap, and routed topologies.

Syntax

```
name <Topology name>
```

Parameters

<Topology name>	Specifies the name of the topology.

Examples

The following example changes the name of the topology to bridged_ac2.

```
EWC.enterasys.com:topology:bridged_ac1# name bridged_ac2
```

21.4.7 show

Use the **show** command to display information about a topology. The **show** command is available from the **topology:<named-topology>** context of the CLI for admin, b@ac, b@ap, physical, and routed topologies.

Syntax

show

Parameters

None

Examples

The following examples shows configuration information for an admin topology.

```
EWC.enterasys.com:topology:Admin# show
Name: Admin
```

The following example shows configuration information for a b@ac topology.

```
EWC.enterasys.com:topology:Enterasys# show
Synchronize: disable
Name: Enterasys
Layer 3 presence: disable
```

The following example shows configuration information for a b@ap topology.

```
EWC.enterasys.com:topology:BridgedAP2# show
Synchronize: enable
Name: BridgedAP2
```

The following example shows configuration information for a physical topology.

```
EWC.enterasys.com:topology:esa0# show
Name: esa0
3rd party: disable
```

The following example shows configuration information for a routed topology.

```
EWC.enterasys.com:topology:r1# show
Topology mode: routed
Synchronize: enable
Name: r1
```

21.4.8 strict-subnet

Use the **strict-subnet** command to enable or disable strict subnet adherence on a b@ac topology. The **strict-subnet** command is available from the **topology:<named-topology>** context of the CLI for b@ac topologies.

Syntax

```
strict-subnet enable | disable
```

Parameters

enable	Enables strict subnet adherence.
disable	Disables strict subnet adherence.

Examples

The following example enables strict subnet adherence on a b@ac topology.

```
EWC.enterasys.com:topology:bridged_ac1# strict-subnet enable
```

21.4.9 sync

Use the **sync** command to enable or disable automatic synchronization of this topology across paired controllers. The **sync** command is available from the **topology:<named-topology>** context of the CLI for b@ac, b@ap, and routed topologies.

Syntax

```
sync enable | disable
```

Parameters

enable	Enables synchronization.
disable	Disables synchronization.

Examples

The following example enables synchronization.

```
EWC.enterasys.com:topology:r1# sync enable
```

22

Location Commands (lbs)

This section describes commands used to enable and configure an AeroScout location based service on a Enterasys Wireless Controller and Wireless APs. These commands are located in the **lbs** context of the CLI. Execute the **lbs** command at the root level to enter **lbs** context.

Note: All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the **lbs** context:

- service
- server-ip
- show

For information on related commands that are available in other contexts, see "Related commands" on page 22-2.

22.1 service

Use the **service** command to enable or disable the AeroScout location based service on the Enterasys Wireless Controller. The **service** command is accessible from the **lbs** context of the CLI.

Syntax

```
service enable|disable
```

Parameters

enable|disable	Specifies the name of the topology.

Usage

You must also use the **server-ip** command specify the IP address of the AeroScout server.

Examples

The following example enables the AeroScout location based service.

```
EWC.enterasys.com:lbs# service enable
```

22.2 server-ip

Use the **server-ip** command to set the AeroScout IP address. The **server-ip** command is accessible from the **lbs** context of the CLI.

Syntax

```
server-ip A.B.C.D
```

Parameters

A.B.C.D	Specifies the IP address of the AeroScout server.

Usage

This command is visible only if you have set the **service** command to enable.

The default IP address is 0.0.0.0.

Examples

The following example sets the IP address of the AeroScout server to 192.168.3.100.

```
EWC.enterasys.com:lbs# server-ip 192.168.3.100
```

22.3 show

Use the **show** command to display information about the AeroScout location based service. The show command is accessible from the **lbs** context of the CLI.

Syntax

show

Parameters

None.

Examples

The following example displays information for the AeroScout location based service.

```
EWC.enterasys.com:lbs# show
LBS server: 192.168.3.100
LBS status: enable
```

22.4 Related commands

The following commands in other contexts relate to the AeroScout location based service:

- lbs-status
- show

22.4.1 lbs-status

The **lbs-status** command allows you to enable or disable the collection of AeroScout tags on a specific 802.11n AP or all 802.11n APs.

The **lbs-status** command is accessible from the following contexts:

- **ap:<serial>** — Use the **lbs-status** command in this context to enable or disable the collection of AeroScout tags on a specific 802.11n AP. See "lbs-status" on page 4-148.
- **ap:defaults:11n** — Use the **lbs-status** command in this context to enable or disable the collection of AeroScout tags on all 802.11n APs. See "lbs-status" on page 4-7.

22.4.2 show

The **show** command allows you to display configuration information, including lbs-status, for a specific 802.11n AP or all 802.11n APs.

The **show** command is accessible from the following contexts:

- **ap:<serial>** — Use the **show** command in this context to display configuration information for a specific 802.11n AP. See "show" on page 4-153.
- **ap:defaults:11n** — Use the **show** command in this context to display configuration information for a all 802.11n APs. See "show" on page 4-41.

23

web Commands

The **web** command refers to the web context, which contains commands used to configure the web settings. The **web** command is accessible from the root context of the CLI.

The following commands are available in the **web** context:

- guestportal-admin-timeout
- timeout
- showvns
- show

23.1 guestportal-admin-timeout

Use the **guestportal-admin-timeout** command to configure the time after which the web sessions of guest administrator users (guestportal user type) will time out. The **guestportal-admin-timeout** command is accessible from the **web** context of the CLI.

Syntax

```
guestportal-admin-timeout <xx:xx> (hour:minutes or just minutes, range 1 minute
to 7 days)
```

Parameters

<xx:xx>	Specifies time in hh:mm format

Examples

The following example sets the web session timeout to one hour and 30 minutes.

```
EWC.enterasys.com:web# guestportal-admin-timeout 01:30
```

The following example sets the web session timeout to 30 minutes.

```
EWC.enterasys.com:web# guestportal-admin-timeout 00:30
```

Note: After you have run the **guestportal-admin-timeout** command, you must run the **apply** command to implement the changes.

23.2 timeout

Use the **timeout** command to configure the time after which the web session will time out. The **timeout** command is accessible from the **web** context of the CLI.

Syntax

```
timeout <xx:xx> (hour:minutes or just minutes, range 1 minute to 7 days)
```

Parameters

<xx:xx>	Specifies time in hh:mm format

Examples

The following example sets the web session timeout to one hour and 30 minutes.

```
EWC.enterasys.com:web# timeout 01:30
```

The following example sets the web session timeout to 30 minutes.

```
EWC.enterasys.com:web# timeout 00:30
```

Note: After you have run the **timeout** command, you must run the **apply** command to implement the changes.

23.3 showvns

Use the **showvns** command to display the VNS names in the Wireless AP SSID list on the controller's user interface (Wireless AP screen). Use the **no** form of the command to remove the VNS names in the Wireless AP SSID list. The **showvns** command is accessible from the **web** context of the CLI.

Syntax

```
showvns
no showvns
```

Parameters

None

Examples

The following example displays the VNS names in the Wireless AP SSID list on the controller's user interface (Wireless AP screen).

```
EWC.enterasys.com:web# showvns
```

The following example removes the VNS names in the Wireless AP SSID list on the controller's user interface (Wireless AP screen).

```
EWC.enterasys.com:web# no showvns
```

Note: After you have run the **showvns** command, you must run the **apply** command to implement the changes.

23.4 show

Use the **show** command to display the web settings.

Syntax

```
show
```

Parameters

None

Examples

The following example displays the web settings.

```
EWC.enterasys.com:web# show
timeout 34:0
showvns
```

24

Wireless AP Diagnostics

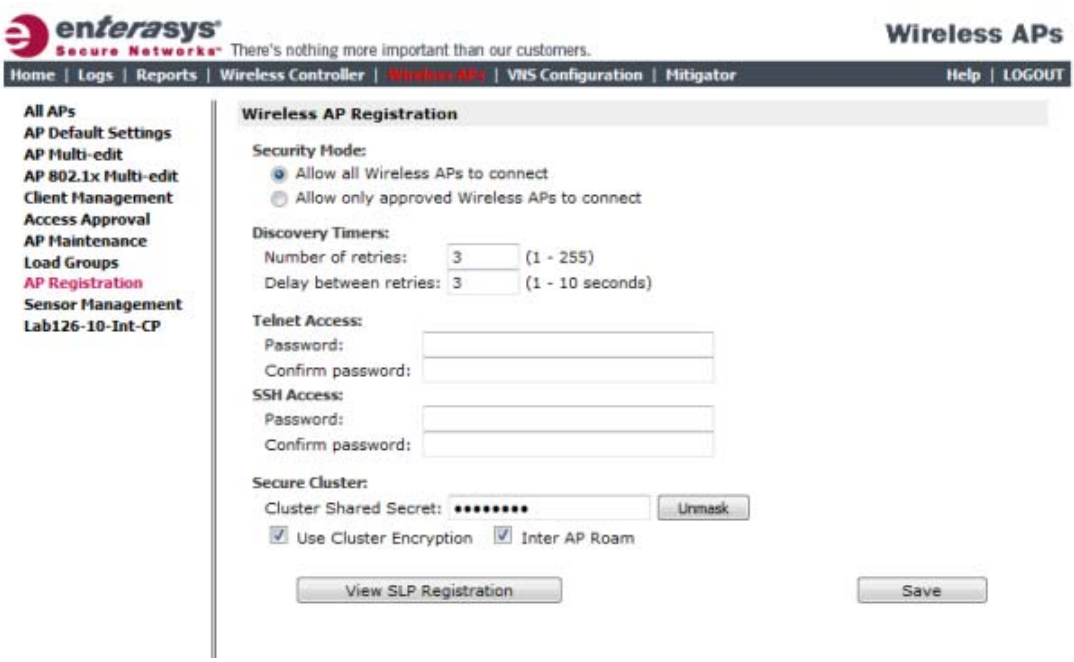
Performing Wireless AP Diagnostics Using Telnet

Caution: For security reasons, telnet is disabled by default. Telnet should only be enabled to perform diagnostic sessions. When completed, telnet should always be disabled.

As a support tool to perform diagnostic debugging of the Wireless AP, the capability to access the Wireless AP by telnet has been provided. Normally, telnet is disabled and should be disabled again after diagnostics. This process should only be used by support services.

To enable telnet access:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen appears.
2. From the left pane, click **AP Registration.** The **Wireless AP Registration** screen appears.



3. In the **Telnet Access** area, in the **Password** box, type the password for a Telnet session.
4. To confirm the password, in the **Confirm Password** box, re-type the password.

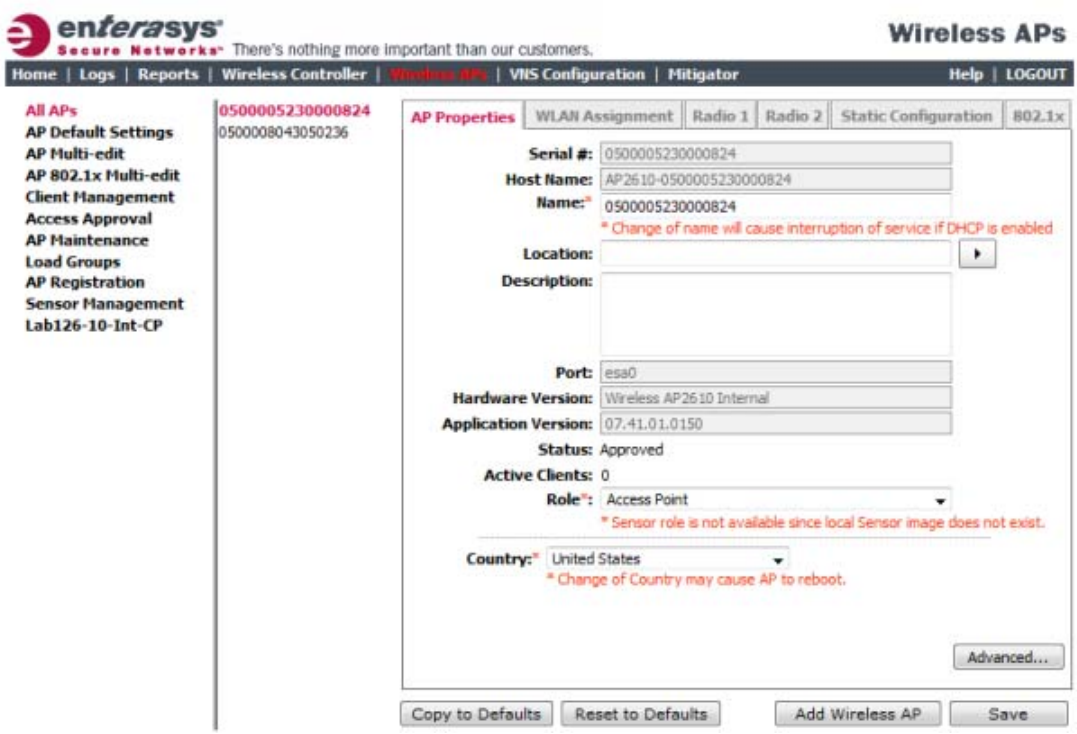
Note: When the Enterasys Wireless Controller ships from the factory it is configured with a default password to assign to the Wireless APs that register with it. The default password is **new2day**. The password is sent to the Wireless APafter it has registered. The administrator can override this password using the Wireless AP Registration page in the GUI. For more information, see the Enterasys Wireless Controller, *Access Points and Convergence Software User Guide*.

5. To send the password information to all registered Wireless APs, click **Save**.

Note: The admin password is modified in the Wireless AP when a new password is saved for telnet access.
Telnet to Wireless APs works via the Enterasys Wireless Controller console port only.

To enable telnet on a selected Wireless AP:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen appears.
2. In the Wireless AP list, click the Wireless AP for which you want to enable telnet. The **Wireless AP Properties** screen appears.



3. Click on the **Advanced** button.
4. From the **Telnet Access** drop-down list, click **Enable**.
5. Click **Save**. This Wireless AP is enabled for a telnet session.

To disable Telnet access:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen appears.
2. In the Wireless AP list, click the Wireless AP for which you want to enable telnet. The **Wireless AP Properties** screen appears.
3. Click on the **Advanced** button, then from the **Telnet Access** drop-down list, click **Disable**.
4. Click on the **Save** button. The Wireless AP is disabled for the telnet sessions.